ESCUELA SUPERIOR POLITECNICA DE CHIMBORAZO

"PROPUESTA DE UN METODO ALTERNATIVO DE ENCRIPTACIÓN DINAMICA PARA UN ADMINISTRADOR DE CORREO ELECTRONICO"

Tesis de Grado previo a la obtención del grado de

MASTER EN INFORMÁTICA APLICADA

Autor:

Ing. Danilo Pastor

Riobamba – Ecuador

INDICE GENERAL

INDICE DE GRAFICOS

INDICE DE TABLAS

ABREVIATURAS

ACL	Access Control List. Lista de Control de Acceso
AES	Advanced Encryption Standard. Norma de encriptación avanzada
AU	Agente de Usuario
DES	Data Encryption Standard. Norma de encriptación de datos.
DHCP	Dinamic Host Confiration Protocol. Protocolo de Configuración Dinámica de Host
DNS	Domain Name System. Sistema de Nombres de dominio
E-MAIL	Electronic Mail. Correo Electrónico
IDEA	Internacional Data Encryption Algorithm. Algoritmo de encriptación de datos Internacional
HTML	Hypertext Markup Language. Lenguaje de marcas hipertextual
HTTP	Hipertext Transfer Protocol. Protocolo de Tranferencia de hipertexto
IETF	Internet Engineering Task Force. Grupo de normalización de Ingeniería en Internet
IMC	Internet Mail Consorcium. Consorcio de Correo en Internet
IP	Internet Protocol. Protocolo Internet
MIME	Multipurpose Internet Mail Extensions. Extensiones de Correo en Internet multipropósito.
MTA	Mail Transfer Agent. Agente de Tranferecnia de Correo
OSI	Open System Interconnection. Interconexión de Sistemas Abiertos
PAP	Password Authentication Protocol. Protocolo de autentificación de password
PKI	Public Key Infrastruture. Infraestructura de Clave Pública.

PKCS	Public-key Cryptographic Standard. Estándar de Criptografía de Clave Pública
POP	Postal Office protocol. Protocolo de Oficina Postal
RFC	Request for Comments. Solicitudes de Comentarios
RPC	Remote Procedure Call. Llamada a procedimiento remoto
SID	Security Identification. Identificador de Seguridad.
SMTP	Simple Mail Tranfer Protocol. Protocolo Básico de Transferencia de Correo
SNMP	Simple Network Management Protocol. Protocolo Básico de Gestión de Red.
SSL	Secure Sockets Layer. Protocolo de Comunicaciones Seguras
SUID	Set User Identification. Conjunto de Identificación de Usuario
TCP/IP	Transfer Control Protocol / Internet protocol. Protocolo de Control de Transmisión / Protocolo Internet
UML	Unified Modeling Language. Lenguaje de Modelado Unificado.
URL	Uniform Resource Locator. Localizador Universal de Recursos

INTRODUCCION

El correo electrónico es, de los servicios que proporciona Internet, sin duda el más utilizado, tanto por volumen de información transmitida, como por número de usuarios que habitualmente lo utilizan. Sin embargo**,** se tiene idea sobre la privacidad y seguridad de la información que se envía y recibe a través del e-mail. Curiosamente, los navegadores de Internet suelen mostrar un aviso acerca de la posibilidad de que los datos que se envíen a través de un formulario electrónico, por ejemplo una búsqueda, pueden ser vistos por otros, pero es raro encontrar una advertencia como ésta en los clientes de correo electrónico.

La realidad es que un e-mail, pasa por un número indeterminado de máquinas hasta llegar a su destinatario final. Cada uno de los administradores de estos equipos, situados en cualquier lugar del mundo podría, si lo desea, acceder a la información. De ellos, los que mayor interés podrían tener en la revisión de nuestro e-mail son precisamente los primeros de la cadena, si utilizamos el sistema de correo de la empresa o cliente para el que estamos trabajando, por ejemplo. Además, se debe considerar que los datos enviados a través de un correo electrónico; el nombre y apellidos, o al menos las direcciones de e-mail, tanto del emisor, receptor y posibles destinatarios de copias del mensaje, forman parte de la transmisión y por lo tanto están expuestas a la intercepción de esta información.

Por lo tanto la información contenida en los mensajes de correo electrónico suelen circular por la red en formato texto, a la vista de demasiados intermediarios**.** Por lo que se hace necesario que la información sensible o confidencial se distribuya de manera segura a sus destinatarios. Para ello, la presente investigación propone una alternativa de solución, que consiste en que la comunicación

entre el cliente y el Servidor se lo haga encriptando la información. Cada texto que hay que transmitir entre uno y otro usuario se lo realiza transformándolo según una clave que se genera dinámicamente, siendo desencriptada al llegar a su destino.

La encriptación garantiza que la información no sea inteligible para individuos, entidades o procesos no autorizados. Consiste en transformar un texto en claro mediante un método de cifrado en un texto encriptado, gracias a la información secreta o clave de cifrado. Como en la investigación se propone un criptosistema simétrico, se supone que la misma clave emplea el Emisor así como el Receptor.

Se propone un método alternativo de encriptar mensajes de correo electrónico debido a que los Clientes de Correo tradicionales no incluyen características inherentes de encriptación, a menos que se utilice infraestructura de clave pública, la cual necesita disponer de certificados digitales emitidos por una entidad certificadora. Entonces en la presente investigación se desarrolla un Software Cliente de Correo que incorpora propiedades intrínsecas de cifrado automáticamente y transparente para el usuario sin necesidad de recurrir a terceros.

DESCRIPCION DEL TRABAJO

Para cumplir con los objetivos del presente trabajo de investigación, se lo ha dividido en seis capítulos:

El Primer Capítulo ***Marco Referencial***, describe la problematización de la investigación, su justificación y los objetivos generales y específicos planteados, con los cuales se quiere llegar a los resultados que se esperan obtener con la investigación para resolver el problema.

El Segundo Capítulo ***Marco Teórico***, realiza una descripción de los antecedentes, conceptos y la teoría relacionada a la Criptografía, Protocolos y Estándares de Transmisión de Correo Electrónico.

El Tercer Capítulo ***Marco Metodológico,*** incluye el planteamiento del sistema de hipótesis y su respectiva operacionalización de las variables. Además se menciona el diseño de la investigación, se determina la Población y Muestra, se justifica los Instrumentos y técnicas de recolección de datos con su respectiva validación.

El Cuarto Capítulo contempla el ***Análisis e Interpretación de Resultados,*** en el cual se describe todo el procesamiento de la información tanto para la variable Independiente como para la variable Dependiente. Se contempla al final del capítulo la interpretación de los resultados obtenidos en cada variable.

El Quinto Capítulo ***Marco Propositivo***, describe detalladamente el método de encriptación dinámica propuesto como objetivo de la investigación.

El Sexto Capítulo ***Desarrollo de un Prototipo Cliente de Correo Electrónico***, describe todo el proceso de desarrollo de software un Cliente de Correo Electrónico propuesto como objetivo de la investigación

Finalmente se llega a describir las ***Conclusiones y Recomendaciones,*** se incluyen los resultados y sugerencias finales del trabajo de investigación.

CAPITULO I

MARCO REFERENCIAL

1.1 TEMA

"PROPUESTA DE UN METODO ALTERNATIVO DE ENCRIPTACIÓN DINAMICA PARA UN ADMINISTRADOR DE CORREO ELECTRONICO"

1.2 PLANTEAMIENTO DEL PROBLEMA

Los sistemas de comunicación se utilizan para transmitir datos y por ende las preocupaciones de disponibilidad, seguridad e integridad son importantes para evitar las amenazas. El objetivo del agresor es obtener la información que se esté transmitiendo. La amenaza de revelación del contenido de mensajes por correo electrónico o un archivo transferido pueden contener información delicada o confidencial.

Se desea evitar que los agresores conozcan el contenido de estas transmisiones mediante un método de encriptación particular.

También se puede indicar que todos los software de administración de correo solo muestran la información que ha sido transmitida o recibida sin prestar protección.

Además todos los usuarios que utilizan el servicio de correo electrónico se confían que la información que ellos manipulan es segura y no existen agresores o personas que puedan alterar la información.

Los sistemas criptográficos clásicos están presentando una dificultad en cuanto a la relación complejidad-longitud de la clave / tiempo necesario para encriptar y desencriptar el mensaje.

Las principales desventajas de los métodos simétricos son la distribución de las claves, el peligro de que muchas personas deban conocer una misma clave y la dificultad de almacenar y proteger muchas claves diferentes. La clave es corta, tanto que no asegura una fortaleza adecuada. Hasta ahora había resultado suficiente, y nunca había sido roto el sistema. Pero con la potencia de cálculo actual y venidera de los computadores y con el trabajo en equipo por Internet se crée que se puede violar el algoritmo, como ya ha ocurrido una vez, aunque eso sí, en un plazo de tiempo que no resultó peligroso para la información cifrada.

1.3 JUSTIFICACION DE LA INVESTIGACION

La preocupación de la confidencialidad es, por supuesto, la lectura no autorizada de mensajes o archivos que navegan en todo el mundo de Internet. Este campo ha sido objeto de muchas investigaciones las cuales buscan cuidar la integridad de la información para evitar consecuencias poco trascendentes o desastrosas.

La presente Investigación trata de solucionar uno de los problemas más comunes en la comunicación a través de Internet. La inseguridad que existe en el tratamiento de la información,

especialmente en el servicio de correo electrónico y básicamente en la emisión de mensajes y archivos suelen ser alterados, violados o simplemente se puede ver la información cosa que compromete la confidencialidad de la información.

Se trata de utilizar técnicas, métodos innovadores de encriptación dinámicos en base a parámetros de que cambien constantemente tales como días de año, horas del día, zona horarias, ubicaciones, y más, que se acoplen a la realidad actual de tal forma de garantizar y asegurar que la información transmitida pueda ser confiable en cualquiera de los puntos en donde se cuente la alternativa propuesta.

En la actualidad los administradores de correo normalmente no utilizan características de encriptación por defecto, ya que si se desean ciertos niveles de seguridad hay que pagar por firmas digitales y otros medios pagados. La investigación propuesta ayudará a utilizar un gestor de correo en forma segura ya que por defecto incluye características de seguridad pasando por desapercibido por el usuario final.

Finalmente vale la pena considerar que la investigación puede ser muy importante ya que el ámbito de la seguridad en la actualidad se convierte en un tema de estudio muy profundo y de mucha dedicación que podría ser aplicada a otras áreas similares como la web, y en la redes sobre TCP/IP.

1.4 OBJETIVOS DE LA INVESTIGACION

1.4.1 OBJETIVO GENERAL

- Desarrollar un método alternativo de encriptación para la transmisión de información de un administrador de correo electrónico y así garantizar la confiabilidad y seguridad en la transmisión de mensajes.

1.4.2 OBJETIVOS ESPECIFICOS

- Proponer un método particular de cifrado dinámico que sea diferente a los convencionales que se sujeten a los estándares ya existentes y que garanticen la protección de la información.

- Desarrollar un software prototipo que gestione el uso de correo electrónico encriptando la transmisión de mensajes para demostrar la seguridad de la información mediante el uso del método dinámico propuesto.

CAPITULO II

MARCO TEORICO

2.1 INTRODUCCION A LA CRIPTOGRAFIA

Para establecer una comunicación de datos entre dos entidades (personas, equipos informáticos, etc) hacen falta al menos tres elementos básicos: el emisor del mensaje (la fuente), el receptor del mismo (el destino) y un soporte físico por el cual se transfieran los datos (el medio).

En una comunicación normal los datos se envían a través del medio tal como son, sin sufrir modificaciones de ningún tipo, de tal forma que el mensaje que representan puede ser interceptado y leído por cualquier otra entidad que acceda a él durante su viaje por el medio.

Pero hay ocasiones en las que nos interesa que dicho mensaje solamente pueda ser interpretado correctamente por el emisor del mismo y por el receptor al que va dirigido. En estas ocasiones es necesario implementar algún mecanismo de protección de la información sensible tal que el mensaje viaje seguro desde la fuente al destino, siendo imposible la interceptación por terceros del mensaje, o que si se produce ésta, el mensaje capturado sea incomprensible para quien tenga acceso al mismo.

Una de las formas de conseguir esto es enviar el mensaje en claro, tal como lo ha redactado el emisor, y pretejerlo en el camino mediante sistemas de fuerza que lo defiendan durante el camino, como es el caso de la protección de mensajes mediante personal de seguridad.

Otro método posible es el enviar el mensaje por un camino con tanto tráfico de información que resulte muy difícil a las terceras personas detectar que se trata de información confidencial (la mejor forma de ocultar un árbol es dentro de un bosque), como es el caso de enviar el mensaje mediante una carta por el sistema estándar de correo.

Desafortunadamente estos métodos de protección de mensajes, al igual que otros análogos, han demostrado su inefectividad a lo largo de los tiempos, por lo que hubo que buscar otro tipo de mecanismos para proteger la información sensible en su camino entre emisor y receptor.

La criptografa ha demostrado con el tiempo ser una de las mejores técnicas para resolver esta cuestión. Tanto es así que actualmente, en la época de los ordenadores y la información, es el mecanismo más usado en los procesos de protección de datos, como las transacciones bancarias por Internet, el correo electrónico cifrado, etc.

Esto es así porque es tal vez el único medio asequible y fácil de implementar para lograr un acceso controlado a la información en un medio, Internet, que por su propia naturaleza es abierto y de acceso libre a la información.

Tanta ha sido la importancia de los sistemas criptográficos que, por ejemplo, en la Segunda Guerra Mundial la famosa máquina alemana ENIGMA trajo en jaque durante mucho tiempo al ejército aliado, al permitir a los nazis el envío de información cifrada a sus tropas. Y en la actualidad los sistemas de cifrado están financiados en su mayoría por los gobiernos y sus militares, constituyendo el resultado de las investigaciones materia reservada.

2.2 DEFINICION DE CRIPTOGRAFIA

Entendemos por Criptografía (Kriptos=ocultar, Graphos=escritura) la técnica de transformar un mensaje inteligible, denominado **texto en claro**, en otro que sólo puedan entender las personas autorizadas a ello, que llamaremos **criptograma** o texto cifrado. El sistema empleado para encriptar el texto en claro se denomina **algoritmo de encriptación**.

La Criptografía es una rama de las Matemáticas, que se complementa con el Criptoanálisis, que es la técnica de descifrar textos cifrados sin tener autorización para ellos, es decir, realizar una especie de Criptografía inversa. Ambas técnicas forman la ciencia llamada Criptología.

La base de las Criptografía suele ser la aplicación de problemas matemáticos de difícil solución a aplicaciones específicas, denominándose **criptosistema** o **sistema de cifrado** a los fundamentos y procedimientos de operación involucrados en dicha aplicación.

2.2.1 CRITOGRAFIA CLASICA

El cifrado de textos es una actividad que ha sido ampliamente usada a lo largo de la historia humana, sobre todo en el campo militar y en aquellos otros en los que es necesario enviar mensajes con información confidencial y sensible a través de medios no seguros.

Aunque en cierta forma el sistema de jeroglíficos egipcio puede considerarse ya una forma de criptografía (sólo podían ser entendidos por personas con conocimientos suficientes), el primer sistema criptográfico como tal conocido de debe a Julio César. Su sistema consistía en reemplazar en el mensaje a enviar cada letra por la situada tres posiciones por delante en el alfabeto latino. En nuestro alfabeto actual tendríamos la siguiente tabla de equivalencias:

A	B	C	D	E	F	G	H	I	J	K	L	M	N	Ñ	O	P	Q	R	S	T	U	V	W	X	Y	Z
D	E	F	G	H	I	J	K	L	M	N	Ñ	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C

Por lo que el mensaje "HOLA MUNDO" se transformaría en "KRÑD OXPGR". Para volver al mensaje original desde el texto cifrado tan sólo hay que coger un alfabeto e ir sustituyendo cada letra por la que está tres posiciones antes en el mismo.

Este sistema fue innovador en su época, aunque en realidad es fácil de romper, ya en todo sistema de transposición simple sólo hay un número de variaciones posible igual al de letras que formen el alfabeto (27 en este caso).

Este fue el primer sistema criptográfico conocido, y a partir de él, y a lo largo de las historia, aparecieron otros muchos sistemas, basados en técnicas criptológicas diferentes. Entre ellos caben destacar los sistemas monoalfabéticos (parecidos al de Julio César, pero que transforman cada letra del alfabeto original en la correspondiente de un alfabeto desordenado), el sistema Playfair de Ser Charles Wheastone (1854, sistema monoalfabético de diagramas), los sistemas polialfabéticos, los de permutación, etc.

Aunque han sido muchos, y no vamos a verlos a fondo, sí hay que destacar dos sistemas generales de ocultación, ya que juntos forman la base de muchos de los sistemas criptográficos actuales. Son la sustitución y la permutación.

La sustitución consiste en cambiar los caracteres componentes del mensaje original en otros según una regla determinada *de posición natural en el alfabeto*. Por ejemplo, fijar una equivalencia entre las letras del alfabeto original y una variación de él, de forma análoga a lo que ocurre en el método de Julio César. Si fijamos la equivalencia de alfabetos:

A	B	C	D	E	F	G	H	I	J	K	L	M	N	Ñ	O	P	Q	R	S	T	U	V	W	X	Y	Z
J	K	L	M	N	Ñ	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I

El mensaje "HOLA MUNDO" quedaría como "PXTJ UDVMX". No es necesario que el alfabeto equivalente esté ordenado naturalmente, si no que puede estar en cualquier otro orden. Sólo se exige que tenga todos y cada uno de los elementos del alfabeto original.

Este tipo de sustituciones se denomina monoalfabético, pero existen métodos más eficaces, como los poli alfabéticos, en los que existen varios alfabetos de cifrado, que se emplean en rotación.

La transposición en cambio consiste en cambiar los caracteres componentes del mensaje original en otros según una regla determinada *de posición en el orden del mensaje.* Por ejemplo, si establecemos la siguiente regla de cambio en el orden de las letras en el texto:

la letra	1	2	3	4	5	6	7	8	9
Pasa a ser la	5	1	4	7	8	2	9	3	6

la frase "HOLA MUNDO" nos quedaría "OUDL HOAMN".

Tanto la **sustitución** como la **transposición** son técnicas básicas para ocultar la redundancia en un texto plano, redundancia que se transmite al texto cifrado, y que puede ser el punto de partida para un ataque por Criptoanálisis. La redundancia es el hecho de que casi todos los símbolos de un mensaje en lenguaje natural contienen información que se puede extraer de los símbolos que le rodean.

2.2.2 CLAVES

El problema inmediato que se plantea en cualquier sistema complejo, tanto de sustitución como de permutación, es recordar el nuevo orden que hemos establecido para obtener el mensaje camuflado, problema tanto más difícil de resolver cuento más complicado haya sido el sistema elegido.

Una solución sería escribir en un soporte cualquiera (papel, disquete, etc.) este nuevo orden, pero siempre queda entonces el nuevo problema de guardar el soporte, ya que si cae en manos extrañas dará al traste con el mecanismo de ocultación.

Mejor solución es implementar un mecanismo de sustitución o de permutación basado en una palabra o serie fácil de recordar. Por ejemplo, podemos establecer un mecanismo criptográfico que se base en una palabra corta. Consideremos que queremos cifrar la frase "HOLA MUNDO" basándonos en la palabra "HTML". Para ello escribimos una tabla o matriz con tantas columnas como letras tenga la palabra elegida, y colocamos en la fila superior dicha palabra. El mensaje a cifrar lo vamos situando en las filas siguientes consecutivamente y si sobran celdas las dejamos vacías:

H	T	M	L
H	O	L	A
M	U	N	D
O			

El paso siguiente será cambiar el orden de las filas, por ejemplo ordenando la palabra elegida en orden alfabético, con lo que nuestra tabla nos queda:

H	L	M	T
H	A	L	O
M	D	N	U
O			

Por último, podemos transformar las filas de la tabla en columnas:

H	H	M	O
L	A	D	
M	L	N	
O			

Y ya sólo nos queda obtener el nuevo mensaje, leyendo las filas obtenidas:

Transformación: "HOLA MUNDO"--------->"HHMO LAD MLN O".

Para desencriptar el texto cifrado habrá que realizar los operaciones anteriores en sentido inverso.

El uso de una palabra o serie determinada como base de un sistema de cifrado posee la ventaja de que, si el sistema es complejo, tan sólo será fácil obtener el texto en claro a quién sepa dicha palabra, además de ser fácil de recordar. Esta palabra o serie base del mecanismo de cifrado se denomina clave de cifrado, y el número de letras que la forman se llama longitud de la clave.

Indudablemente, cuanto más complicado sea el mecanismo de cifrado y cuanto más larga sea la clave, más difícil será romper el sistema y obtener el mensaje original para un extraño. Pero más complicado será también para el destinatario del mensaje cifrado realizar las operaciones de descifrado y obtener el mensaje original, por lo que se crea el dilema seguridad / tiempo.

Las claves de encriptación van a ser la base fundamental de los modernos sistemas criptográficos, basados en operaciones matemáticas generalmente muy complejas.

2.3 CRITOGRAFIA MODERNA

Como se revisó en el punto anterior, los sistemas criptográficos clásicos presentaban una dificultad en cuanto a la relación complejidad-longitud de la clave / tiempo necesario para encriptar y desencriptar el mensaje.

En la era moderna esta barrera clásica se rompió, debido principalmente a los siguientes factores:

- Velocidad de cálculo: con la aparición de los computadores se dispuso de una potencia de cálculo muy superior a la de los métodos clásicos.
- Avance de las matemáticas : que permitieron encontrar y definir con claridad sistemas criptográficos estables y seguros.
- Necesidades de seguridad: surgieron muchas actividades nuevas que precisaban la ocultación de datos, con lo que la Criptología experimentó un fuerte avance.

A partir de estas bases surgieron nuevos y complejos sistemas criptográficos, que se clasificaron en dos tipos o familias principales, los de clave simétrica y los de clave pública. Los modernos algoritmos de encriptación simétricos mezclan la transposición y la permutación, mientras que los de clave pública se basan más en complejas operaciones matemáticas.

2.3.1 CRITOGRAFIA SIMETRICA

Incluye los sistemas clásicos, y se caracteriza por que en ellos se usa la misma clave para encriptar y para desencriptar, motivo por el que se denomina simétrica.

Figura # 2.1 Encriptación simétrica

Toda la seguridad de este sistema está basada en la llave simétrica, por lo que es misión fundamental tanto del emisor como del receptor conocer esta clave y mantenerla en secreto. Si la llave cáe en manos de terceros, el sistema deja de ser seguro, por lo que habría que desechar dicha llave y generar una nueva.

Para que un algoritmo de este tipo sea considerado fiable debe cumplir varios requisitos básicos:

- Conocido el criptograma (texto cifrado) no se pueden obtener de él ni el texto en claro ni la clave.
- Conocidos el texto en claro y el texto cifrado debe resultar más caro en tiempo o dinero descifrar la clave que el valor posible de la información obtenida por terceros.

Generalmente el algoritmo de encriptación es conocido, se divulga públicamente, por lo que la fortaleza del mismo dependerá de su complejidad interna y sobre todo de la longitud de la clave empleada, ya que una de las formas de criptoanálisis primario de cualquier tipo de sistema es la de prueba-ensayo, mediante la que se van probando diferentes claves hasta encontrar la correcta.
Los algoritmos simétricos encriptan bloques de texto del documento original, y son más sencillos que los sistemas de clave pública, por lo que sus procesos de encriptación y desencriptación son más rápidos.

Todos los sistemas criptográficos clásicos se pueden considerar simétricos, y los principales algoritmos simétricos actuales son DES, **IDEA** y RC5, AES (Advanced Encryption Standart).

Las principales desventajas de los métodos simétricos son la distribución de las claves, el peligro de que muchas personas deban conocer una misma clave y la dificultad de almacenar y proteger muchas claves diferentes.

2.3.2 CRITOGRAFIA DE LLAVE PUBLICA

También llamada asimétrica, se basa en el uso de dos claves diferentes, claves que poséen una propiedad fundamental: una clave puede desencriptar lo que la otra ha encriptado.

Generalmente una de las claves de la pareja, denominada **clave privada**, es usada por el propietario para encriptar los mensajes, mientras que la otra, llamada **clave pública**, es usada para desencriptar el mensaje cifrado.

Las claves pública y privada tienen características matemáticas especiales, de tal forma que se generan siempre a la vez, por parejas, estando cada una de ellas ligada intrínsecamente a la otra, de tal forma que si dos llaves públicas son diferentes, entonces sus llaves privadas asociadas también lo son, y viceversa.

Los algoritmos asimétricos están basados en funciones matemáticas fáciles de resolver en un sentido, pero muy complicadas de realizar en sentido inverso, salvo que se conozca la clave privada, como la potencia y el logaritmo. Ambas claves, pública y privada, están relacionadas matemáticamente, pero esta relación debe ser lo suficientemente compleja como para que resulte muy difícil obtener una a partir de la otra. Este es el motivo por el que normalmente estas claves no las elige el usuario, si no que lo hace un algoritmo específico para ello, y suelen ser de gran longitud.

Mientras que la clave privada debe mantenerla en secreto su propietario, ya que es la base de la seguridad del sistema, la clave pública es difundida ampliamente por Internet, para que esté al alcance del mayor número posible de personas, existiendo servidores que guardan, administran y difunden dichas claves.

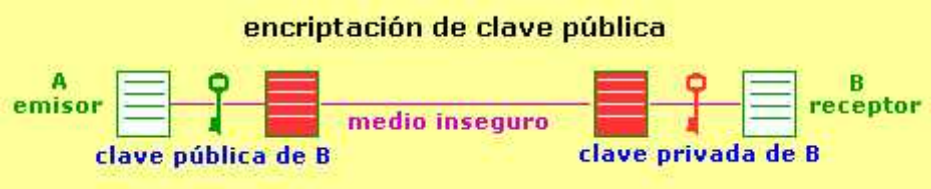


Figura # 2.2 Criptografía de Clave Pública

En este sistema, para enviar un documento con seguridad, el emisor (A) encripta el mismo con la clave pública del receptor (B) y lo envía por el medio inseguro. Este documento está totalmente protegido en su viaje, ya que sólo se puede desencriptar con la clave privada correspondiente, conocida solamente por B. Al llegar el mensaje cifrado a su destino, el receptor usa su clave privada para obtener el mensaje en claro.

Una variación de este sistema se produce cuando es el emisor A el que encripta un texto con su clave privada, enviando por el medio inseguro tanto el mensaje en claro como el cifrado. Así, cualquier receptor B del mismo puede comprobar que el emisor ha sido A, y no otro que lo suplante, con tan sólo desencriptar el texto cifrado con la clave pública de A y comprobar que coincide con el texto sin cifrar. Como sólo A conoce su clave privada, B puede estar seguro de la autenticidad del emisor del mensaje. Este sistema de autentificación de denomina **firma digital**, y lo estudiaremos después con más detenimiento.

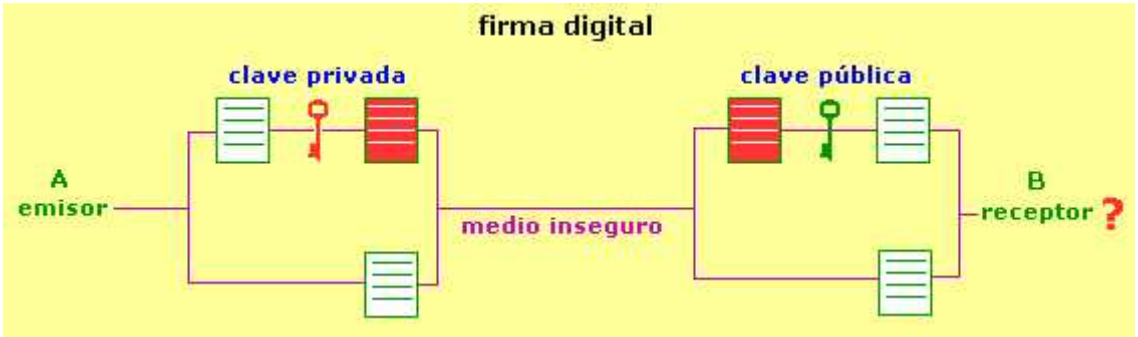


Figura # 2.3 Firma Digital

Para que un algoritmo de clave pública sea considerado seguro debe cumplir:

- Conocido el texto cifrado no debe ser posible encontrar el texto en claro ni la clave privada.
- Conocido el texto cifrado (criptograma) y el texto en claro debe resultar más caro en tiempo o dinero descifrar la clave que el valor posible de la información obtenida por terceros.
- Conocida la clave pública y el texto en claro no se puede generar un criptograma correcto encriptado con la clave privada.
- Dado un texto encriptado con una clave privada sólo existe una pública capaz de desencriptarlo, y viceversa.

La principal ventaja de los sistemas de clave pública frente a los simétricos es que la clave pública y el algoritmo de cifrado son o pueden ser de dominio público y que no es necesario poner en peligro la clave privada en tránsito por los medios inseguros, ya que ésta siempre oculta y en poder únicamente de su propietario. Como desventaja, los sistemas de clave pública dificultan la implementación del sistema y son mucho más lentos que los simétricos.

Generalmente, y debido a la lentitud de proceso de los sistemas de llave pública, estos se utilizan para el envío seguro de claves simétricas, mientras que éstas últimas se usan para el envío general de los datos encriptados.

El primer sistema de clave pública que apareció fue el de **Diffie-Hellman**, en 1976, y fue la base para el desarrollo de los que después aparecieron, entre los que cabe destacar el **RSA** (el más utilizado en la actualidad).

2.4 COMUNICACIÓN SEGURA

En la sociedad actual que nos ha tocado vivir la presencia de los computadores se ha extendido a todos los medios personales, laborales, comerciales, bancarios, etc. Esta presencia ha requerido la aparición y el uso cada vez mayor de los documentos electrónicos, ya sean documentos de texto, hojas de cálculo, ficheros de bases de datos o páginas web seguras. Y en todos los casos ha sido necesaria la implementación de medios seguros de transferencia de estos documentos, lo que se ha conseguido generalmente con el uso de sistemas basados en la criptografía.

Varios son los aspectos que hay que manejar en el proceso de transferencia de un documento electrónico y que definen una comunicación segura:

- Autenticidad: consiste en la seguridad de que las personas que intervienen en el proceso de comunicación son las que dicen ser. Imaginemos que B recibe un documento procedente de A. ¿Cómo está seguro B de que en verdad es A el que se lo ha enviado y no otra persona?.

  Como caso extremo, imagina que te conectas con el sitio web de tu banco par ver el estado de tus cuentas y te aparece la página de entrada de claves de acceso. Esta página tiene el logotipo del banco y un contenido textual en el que se afirma que pertenece a tu banco, pero...¿y si es una imitación de la página real del banco que te ha enviado un servidor pirata para hacerse con tus claves?. El método más usado para proporcionar autenticidad es la firma digital, basada, como no, en la criptografía.

- Confidencialidad: se trata de la seguridad de que los datos que contiene el documento permanecen ocultos a los ojos de terceras personas durante su viaje por el medio desde A a B. Y aquí no entra en juego sólo el papel que realiza la criptografía ocultando los datos, si no también qué se hace con dichos datos una vez han llegado al destinatario de los mismos.

Ataques posibles a la Confidencialidad pueden ser entonces la captura del documento en su viaje de A a B y el uso indebido de los datos del documento o la mala gestión y almacenamiento de estos datos por parte de B. La confidencialidad se consigue generalmente mediante métodos criptográficos.

- Integridad: consiste en la seguridad de que los datos del documento no sufren modificación a lo largo de su viaje por el medio inseguro desde A a B. Un ataque posible a este punto podría ser que una tercera persona capturara el documento en el camino, por ejemplo los datos de un formulario de compra en una tienda virtual, y que los modificara cambiando tu dirección de entrega de los productos por una por él elegida. El banco te haría el cargo de la compra a tí, pero los artículos que has comprado le llegarían al pirata.

  La comprobación de la integridad se suele realizar mediante firmas electrónicas, generalmente basadas en funciones hash.

  La Autenticidad es condición suficiente para la Integridad, por lo que si un documento es auténtico es íntegro, pero no al revés.
- No repudio: se trata de que una vez enviado un documento por A, éste no pueda negar haber sido el autor de dicho envío.

  Imagina que realizas un pedido a una tienda virtual, das tu número de tarjeta de crédito y te cobran los artículos, pero estos no te llegan. Y cuando reclamas a la tienda ésta te dice que ellos jamás han recibido tu pedido. O que la tienda te envía los artículos pedidos y eres tú el que dice luego que no has hecho ningún pedido.

El No repudio es condición sufiente para la Autenticidad, por lo que si un documento es no repudiable es auténtico, pero no al revés.

Cualquier sistema de transferencia segura basado en criptografía debería abarcar estos cuatro aspectos, pero no suelen hacerlo en su totalidad. Así, lo sistemas de clave simétrica ofrecen confidencialidad, pero ninguno de los otros factores, mientras que los sistemas de clave pública ofrecen autenticidad, integridad, confidencialidad en el envío (pero no en las fases posteriores) y no repudio si van asociados a una firma digital.

Otro aspecto a tener en cuenta en lo que se refiere a seguridad en las comunicaciones, aunque se salga del campo de la criptografía, es el de los Servicios de Autorización, que proporciona al usuario acceso solamente a los recursos a los que está autorizado. Esta funcionalidad se suele implementar mediante servidores especiales al efecto, que administran bases de datos con los documentos a los que tiene permitido el acceso cada uno de los usuarios del sistema.

2.5 FUNDAMENTOS MATEMATICOS

Los sistemas criptográficos modernos, tanto si son de clave simétrica como de llave pública, para ser considerados tales deben cumplir una serie de requisitos que los hagan seguros, reversibles y viables. Para obtener sistemas que cumplan estas condiciones se ha desarrollado un campo matemático completo, la Teoría de Códigos, basada en el álgebra de los sistemas discretos y en las clases residuales de módulo dado, que sirve para definir alfabetos y funciones que permiten obtener sistemas robustos.

Generalmente, todo sistema criptográfico se basa en la obtención de un conjunto de elementos, llamados letras o símbolos, que forman un conjunto finito llamado alfabeto fuente, alfabeto fuente y en una función de transformación de dichos símbolos en otros pertenecientes a un conjunto

imagen denominado código. A la función de transformación de le llama función de codificación, f_k, y a las sucesiones finitas de elementos del alfabeto fuente se les denominan palabras. En general, habrá una función de codificación f_k para cada valor de la clave k, definiendo éstas el conjunto de claves del sistema, K.

Si consideramos ahora otro conjunto de símbolos A y el conjunto asociado A* de todas las palabras posibles que se pueden formar con las letras de A, se denomina código C a todo subconjunto finito de éste. Si C está formado por palabras de longitud fija "n", a n se le llama longitud del código C, y a sus elementos n-palabras. Y si C está formado por "m" elementos, se dice entonces que C es un (n,m) código.

Se define un criptosistema como una quíntupla (M,C,K,E,D), donde:

- **M** representa el conjunto de todos los mensajes sin cifrar (texto plano) que pueden ser enviados.
- **C** representa el conjunto de todos los posibles mensajes cifrados (criptogramas).
- **K** representa el conjunto de claves que se pueden emplear en el criptosistema.
- **E** es el conjunto de las transformaciones de cifrado, es decir, el conjunto de funciones matemáticas que se aplican a cada elemento de M para obtener un elemento de C. Existe una transformación diferente E_k para cada valor de la clave k.
- **D** es el conjunto de transformaciones de descifrado, análogo al conjunto E.

Con esta nomenclatura, todo sistema de cifrado debe cumplir la condición:

$$\mathbf{D_k(E_k(m))=m}$$

Para aclarar un poco estos conceptos, vamos a ver un ejemplo basado en nuestro alfabeto castellano. Este sería el alfabeto fuente, las letras (a, b, c, d, e, ...) serían las letras o símbolos del mismo, y las combinaciones de diferentes letras (casa, perro, silla, ...) serán las palabras del alfabeto. Hay que notar que desde un punto de vista matemático y criptográfico también serán palabras dekid, podretyp, lloeer y cualquier otra formada por cualquiera de las letras del alfabeto fuente, no siendo necesario que tengan sentido alguno.

Sea A=alfabeto castellano.

Sea S el alfabeto fuente, subconjunto de A, que es esta caso va a ser S=A, es decir, vamos a considerar como alfabeto fuente todo el alfabeto castellano.

Sea C el código C=A=alfabeto castellano.

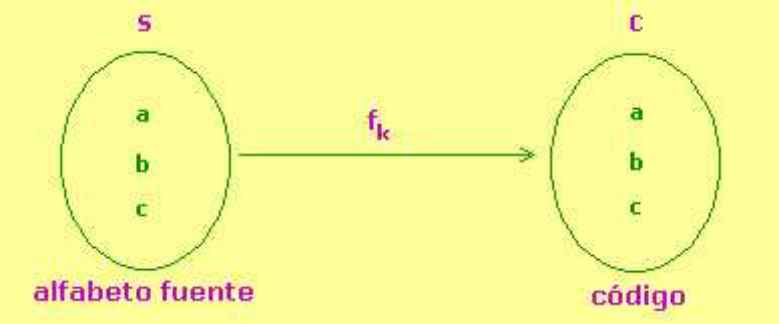


Figura # 2.4 Alfabeto fuente y Código

Definimos nuestra función de codificación, f_1, como: S--f_1-->C, tal que a cada letra le hace corresponder su siguiente en el alfabeto fuente, es decir, la función realizará las siguientes transformaciones:

A	B	C	D	E	F	G	H	I	J	K	L	M	N	Ñ	O	P	Q	R	S	T	U	V	W	X	Y	Z
B	C	D	E	F	G	H	I	J	K	L	M	N	Ñ	O	P	Q	R	S	T	U	V	W	X	Y	Z	A

Consideremos entonces el conjunto M de textos en plano que se pueden formar con las palabras de S, y dentro de él el elemento M_1=HOLA MUNDO. La función de codificación sería en esta caso

$f_1(s)= s+k=s+1$, es decir, la función de cifrado desplaza k posiciones cada letra del alfabeto, siendo en nuestro caso k=1 (k es la clave de cifrado).

Por lo tanto, al aplicar la función f_1 a M_1 tendremos: $f_1(M_1)=f_1$(HOLA MUNDO)=IPMB NVÑEP.

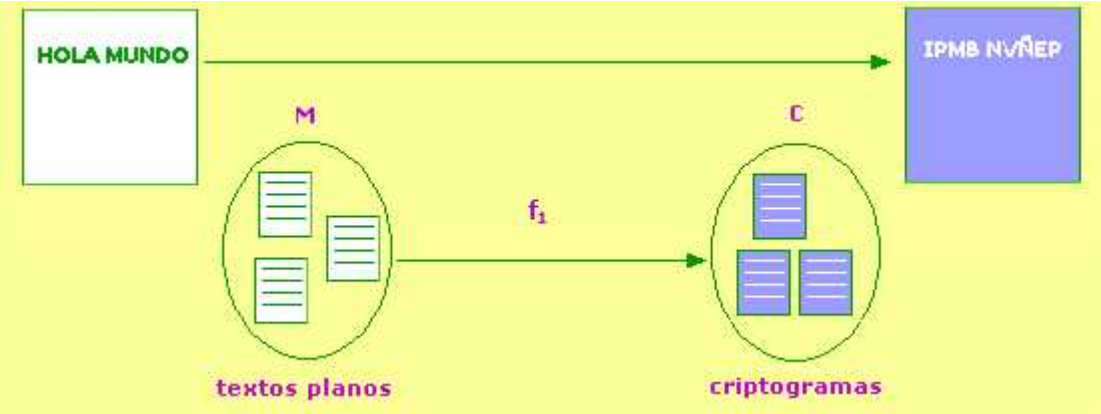


Figura # 2.5 Texto plano y Criptograma

Para que una función pueda ser considerada de codificación debe ser biyectiva, por lo que debe cumplir:

- Elementos diferentes deben tener imágenes diferentes, es decir, no puede haber dos palabras del alfabeto fuente que tengan la misma transformación en el código.
- Todos los elementos deben tener imagen, o lo que es lo mismo, no puede haber palabras del alfabeto fuente que no tengan su transformación en el código.
- No puede haber palabras del código que no se correspondan con alguna palabra del alfabeto fuente.

Estas tres propiedades se resumen diciendo que f debe ser una aplicación uno a uno.

La exigencia de ser biyectiva se traduce en evitar errores, en que la codificación de un mensaje sea única, y su decodificación también. No obstante, muchos sistemas criptográficos implementan una

serie de elementos para la identificación y corrección de errores, ya que durante su viaje por el medio los datos pueden sufrir tales alteraciones que la decodificación resulte incorrecta.

Normalmente las funciones de codificación reales trabajan con números, ya que es la forma que tiene el computador de operar con rapidez, sobre todo teniendo en cuenta que él pasa los números al sistema binario.

Una función de codificación debe ser tal que con ella obtener las imágenes en el código de los elementos del alfabeto fuente sea un proceso simple y rápido, pero la operación contraria, obtener elementos del alfabeto fuente a partir de sus imágenes en el código, si no se conocen ciertos datos (la clave) debe resultar lo más complicado posible. Ese es el verdadero sentido de una buena función de codificación.

La inclusión de las claves en los procesos de encriptación y desencriptación se realiza introduciendo las mismas en los procesos matemáticos pertinentes, generalmente como constantes en la función de codificación. Cuánto más longitud tenga la clave usada, más seguro será el sistema de encriptación y más difícil será romperlo por criptoanálisis, aunque esta fortaleza del cifrado también depende del sistema en sí.

Por ejemplo, los sistemas simétricos tienen, a igualdad de longitud de clave, mucha más fortaleza que los de clave pública. Es por esto que los sistemas simétricos usan 58-128 bits generalmente, mientras que los asimétricos deben manejar claves de más de 512 bits para ser considerados seguros.

* Un último concepto es el de las clases residuales. Dados dos números enteros, a y b, se dice que a es congruente con b módulo n si a y b tienen el mismo resto al ser divididos por n. Por ejemplo, 7 y 10 son congruentes módulo 3, ya que al dividir ambos por 3 nos queda de resto 1.

Con esta consideración, dado un conjunto C se definen sobre él, la clases residuales de módulo n como los subconjuntos de C formados por todos sus elementos tales que al ser divididos por n dan el mismo resto.

Por ejemplo, si C={13,14,15,16,17,18,19} tendremos como clases residuales de módulo 3:

C1={15,18} (al dividirlos entre 3 el resto es 0)

C2={13,16,19} (al dividirlos entre 3 el resto es 1)

C3={14,17} (al dividirlos entre 3 el resto es 2)

Este concepto es importante, ya que muchas de las funciones de codificación usados en los sistemas criptográficos más usados están basadas en las clases residuales del alfabeto fuente.

Para ello manejan la denominada función módulo discreto. De esta forma, a mod(b) representa el resto de dividir a entre b. Si a es inferior a b, tendremos que a mod(b)=a. Vamos a ver algunos ejemplos:

17 mod(6)=5 (ya que 17/6=2 con resto 5)

51 mod(6)=3 (ya que 51/6=8 con resto 3)

4 mod(6)=4 (ya que 4<6)

2.6 ALGORITMO DE ENCRIPTACION “IDEA”

En el congreso Eurocrypt de 1990 fue propuesto el sistema llamado IDEA (Internacional Data Encryption Algorithm). Este cifrado, al igual que el DES, trabaja sobre bloques de 64 bits y presenta el principio de involución, por lo que el descifrado se realiza con el mismo algoritmo que consiste en 8 iteraciones idénticas. En cada una de ellas se usa una subclave diferente, y el bloque

de datos de entrada se divide en 4 subbloques de 16 bits que sufren distintas transformaciones fáciles de implementar.

En el cifrado IDEA se requiere para cada iteración 6 subclaves, y para la transformación de salida 4 más, de forma que en total son necesarias 52 subclaves. La generación de estas subclaves se lleva a cabo mediante una expansión de la clave inicial de 128 bits, de forma que ésta se divide en 8 subclaves de 16 bits que constituyen los 8 primeros subbloques. A continuación se rotan estos cloques de forma circular 25 bits a la izquierda y se obtienen los 8 subbloques, y así sucesivamente.

IDEA garantiza los principios de confusión y difusión, y se considera en general un algoritmo bastante seguro, ya que ha resistido numerosos ataques, entre ellos el criptoanálisis diferencial. Por otra parte. La longitud de clave usada, 128, imposibilita actualmente una búsqueda exhaustiva. Además, hay que decir a su favor que el diseño del algoritmo es más claro que en el caso del DES, ya que cada operación tienen su justificación matemática. También resulta de implementación más eficiente, ya que por una parte no es un algoritmo Feistel, dado que modifican todos los bits en cada iteración y no solo la mitad. Por otra parte, las operaciones utilizadas: XOR, suma módulo 2^{16} y producto $2^{16} + 1$, son fácilmente implementables tanto en hardware como en software.

2.7 ESTANDARES DE CORREO ELECTRONICO

Internet en general y el correo electrónico en particular han tenido una repercusión mundial tan importante en los últimos años debido a la estandarización. Las normas basadas en los protocolos TCP/IP, creadas a través de organismos relacionados con el mundo de la investigación y por empresas, han conseguido imponerse. Sobre todo, a raíz de la popularidad de Internet y del correo electrónico. Describimos las principales normas relacionadas con el correo electrónico de Internet. El IMC (Internet Mail Consorcium) organismo encargado de la normalización de los RFCs para Correo Electrónico plantea los siguientes estándares, expuestos en La Figura # 2.6.

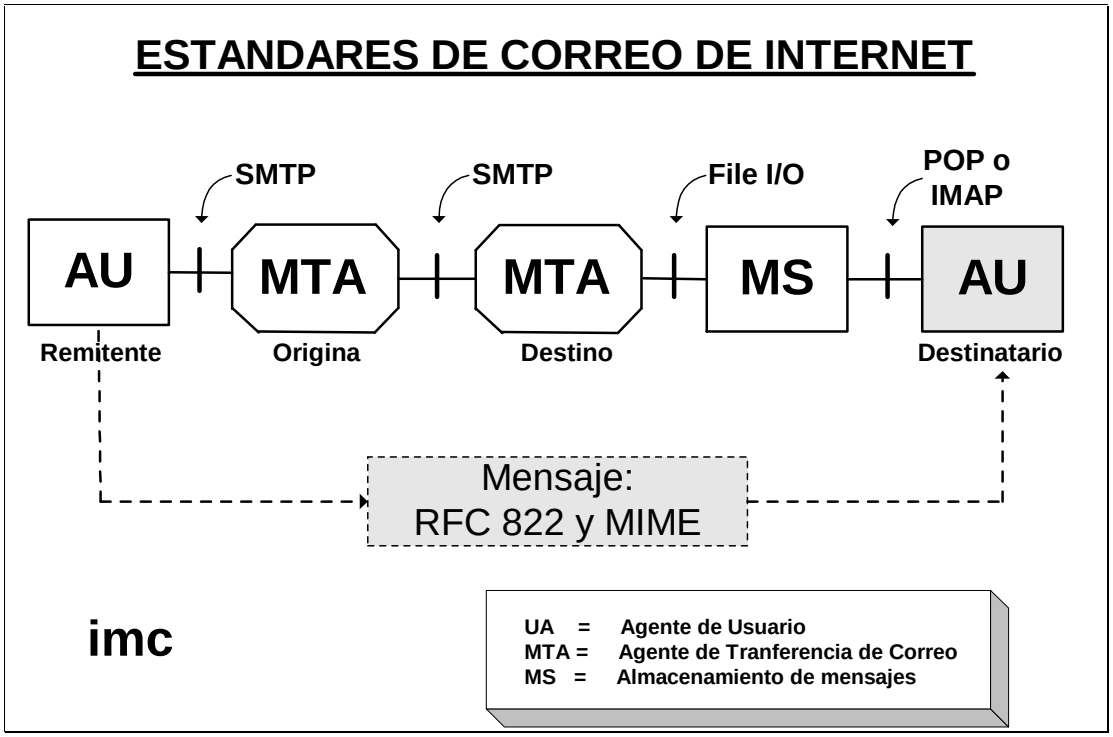


Figura # 2.6 Esquema de IMC sobre los estandares de uso en Internet

A continuación se listan los RFCs relacionados con el correo electrónico en Internet agrupados por varias categorías. Entre los paréntesis se hacen referencia a los protocolos o estándares utilizados para la presente investigación dentro de cada grupo:

- Host-to-host mail transfer (SMTP)
- Client-to-host communication (POP, IMAP)
- Basic message format and encoding (RFC822)
- Multipurpose Internet Mail Extensions (MIME)

2.7.1 Simple Mail Transfer Protocol (SMTP)

El principal mecanismo de transferencia de mensajes en Internet es el protocolo SMTP, que está normalizado en la RFC 821. Garantiza la transferencia de mensajes entre dos servidores que cumplan el protocolo. Pero siempre tienen que iniciar la transferencia a petición del que envía, nunca del que recibe. Es un protocolo muy sencillo pero de gran robustez. El puerto reservado para SMTP en Internet es el 25. La ventaja de tener un servidor de correo centralizado al que accedan

los ordenadores clientes son, básicamente, que no es necesario tener encendido el ordenador del usuario siempre, puesto que éste accede al servidor cada cierto tiempo determinado o a petición del usuario. Otra ventaja es por supuesto de ahorro de costos, el ancho de banda y capacidad del ordenador final sólo tiene que contemplar la conexión con el servidor y no tener en cuenta las posibles conexiones de este ordenador con otros ordenadores de la red.

Finalmente otra ventaja es la posibilidad de conectarse a ese ordenador servidor desde varios ordenadores clientes remotos, independizando el correo de un sitio físico concreto determinado. Por ejemplo, si el servidor se llama dlinux.edigital.com.ec, podremos acceder a él desde cualquier puesto con conexión Internet si así lo permite la política de seguridad de la empresa. El formato de los mensajes que se transfieren a través del protocolo SMTP deben de cumplir la RCF 822. por defecto, deben ser mensajes de 7 bits y los datos de cabecera deben incluir el remitente, el destinatario y la ruta para alcanzar el dominio del destinatario.

2.7.2 Post Office Protocol (POP3)

Existen varias implementaciones diferentes del protocolo. La más extendida actualmente es la conocida como POP3. Es un protocolo diseñado básicamente para conectarse al servidor, identificándole mediante nombre y contraseña y transferir todos los mensajes pendientes desde el servidor al programa cliente del ordenador, borrando los mensajes del servidor. El cliente entregará al servidor SMTP todos los mensajes pendientes de envío. La única información que se puede consultar de los mensajes cuando aún residen en el servidor es su longitud, lo cual puede ser útil si tenemos problemas de espacio en el ordenador donde reside el programa cliente.

El problema más importante con los protocolos POP3 reside cuando consultamos nuestro correo electrónico desde varios ordenadores distintos, puesto que el servidor bajará todos los mensajes pendientes a ese sistema de correo. Por tanto, si se hace uso frecuente de esta posibilidad desde varios servidores nos encontraremos con que podemos tener los mensajes repartidos en varios

ordenadores sin la posibilidad de hacer una gestión común de los mensajes para búsquedas o simplemente ordenar la información. POP3 es un protocolo de recuperación de la información, no de envío de mensajes. Se asume que el cliente intentará enviar los mensajes al servidor mediante SMTP, esto lo consigue mediante unas extensiones al POP3 llamada Xtnd y Xmit.

El protocolo POP3 tiene un uso muy extendido en Internet y lo soportan todos los programas populares que se escogerán en la presente investigación. Debido a esta popularidad es muy difícil que en un futuro cercano sea sustituido por la gran mayoría de usuarios.

CAPITULO III

MARCO METODOLOGICO

3.1 DISEÑO DE LA INVESTIGACION

La presente Investigación se enmarca dentro de un estudio ***cuasiexperimental***, ya que se trabaja con grupos intactos y además se manipula una variable independiente. Su validez se alcanzará a medida que se demuestre las características de los grupos de Clientes de Correo seleccionados, en relación al Software *Propuesto* en la investigación. Por el *Tipo de Datos* es de tipo ***Cuanti-Cualitativo***. Por el tiempo de estudio es de ***Tipo Transversal*** porque se recolectan los datos en un solo momento.

Se ha realizado las siguientes consideraciones para esta investigación:

- Se plantea la investigación en base a los problemas existentes en el área del Correo Electrónico
- Se trazan los objetivos de la investigación que resolverán el problema de la revelación del contenido de mensajes por correo electrónico.
- Se justifica los motivos por los cuales se propone realizar la presente investigación.

- Se elabora un marco teórico que ayude a tener una idea general para la realización del trabajo y un horizonte más amplio.
- Se plantea una hipótesis la cual es una posible repuesta al problema planteado y posee una íntima relación entre el problema y el objetivo.
- Se desarrolla la propuesta del software Procopio en base la método planteado de tal forma que resuelva la confidencialidad de la información que se transmite por correo electrónico.
- Se propone la operacionalización de las variables en base a la hipótesis planteada.
- Se define las unidades de análisis y se delimita la población que va a ser comparada en relación a la propuesta de la investigación.
- Se realiza la recolección de datos de los índices e indicadores respectivos mediante la observación directa y los tests.
- Se realiza la prueba de la hipótesis con los resultados obtenidos.
- Se elabora las conclusiones y recomendaciones producto de la investigación realizada.

3.2 SISTEMA DE HIPOTESIS

EL MÉTODO ALTERNATIVO DE ENCRIPTACIÓN PARA LA TRANSMISIÓN DE INFORMACIÓN DE UN ADMINISTRADOR DE CORREO ELECTRÓNICO FORTALECERÁ LA SEGURIDAD EN LA TRANSMISIÓN Y RECEPCIÓN DE MENSAJES.

3.3 OPERACIONALIZACION DE VARIABLES

De acuerdo a la hipótesis planteada se han identificado dos variables:

- **Variable Independiente:**
    - Método alternativo de encriptación para la transmisión de información de un administrador de correo electrónico

- **Variable Dependiente:**

- Seguridad en la transmisión y recepción de mensajes

La operacionalización metodológica de las variables se muestra en la Tabla No. 3.1

OPERACIONALIZACION DE VARIABLES				
HIPOTESIS	**VARIABLES**	**INDICADORES**	**INDICES**	**INSTRUMENTOS**
El método alternativo de encriptación para la transmisión de información de un administrador de correo electrónico fortalecerá la seguridad en la transmisión y recepción de mensajes	**V. INDEPENDIENTE:** Método alternativo de encriptación para la transmisión de información de un administrador de correo electrónico	Generación de la clave	1. Existe algún tipo de generación de clave 2. Se evita la repetición de las claves de sesión. 3. Grado de seguridad para evitar que el agresor conozca la forma de distribuir la clave. 4. Forma de variabilidad para producir la clave.	• Observación • Cliente de correo • Cliente de correo • Cliente de correo
		Encubrimiento de la clave	5. Existencia de algún tipo de difusión en la clave generada. 6. Existencia de algún tipo de confusión en la clave generada	• Observación directa • Observación directa
		Características de la encriptación	7. Se encripta los mensajes de correo sin interactuar constantemente el usuario 8. Velocidad de encriptación en relación a otros procesos de encriptación asimétricos	• Observación directa • Cliente de correo
		Particularidades del Cliente de Correo Electrónico	9. Existe un método embebido de encriptación en el cliente de correo. 10. Permanecen los mensajes siempre en servidor evitando el contagio de virus. 11. Admite libertad de escoger encriptación o no por parte del usuario 12. Nivel de transparencia para el usuario del proceso de encriptación.	• Cliente de correo • Cliente de correo • Cliente de correo • Encuesta

Tabla # 3.1 Operacionalización de variables – Variable Independiente

OPERACIONALIZACION DE VARIABLES				
HIPOTESIS	**VARIABLES**	**INDICADORES**	**INDICES**	**INSTRUMENTOS**
El método alternativo de encriptación para la transmisión de información de un administrador de correo electrónico fortalecerá la seguridad en la transmisión y recepción de mensajes	**V. DEPENDIENTE:** Seguridad en la transmisión y recepción de mensajes	Confidencialidad	1. Se utiliza cifrado de mensajes 2. Se garantiza el acceso a la información solo al usuario receptor sin utilizar PKI 3. Se evita la revelación de contenido utilizando otros administradores de correo.	• Cliente de correo • Servidor de correo • Clientes de correo comerciales
		Gestión de claves	4. Tamaño de la clave de al menos 128 bits 5. Se evita la repetición de las claves de sesión 6. Riesgo de evitar que el agresor conozca la forma de distribuir la clave 7. Se genera la clave diferente instantáneamente. 8. Existencia de algún tipo de difusión y confusión en la clave generada	• Algoritmo utilizado • Observación directa • • Observación directa • Observación directa • Observación directa
		Algoritmo de encriptación	9. Utiliza algún algoritmo simétrico. 10. Utiliza algún algoritmo asimétrico 11. Velocidad de encriptación del algoritmo. 12. Tiene popularidad de aceptación el algoritmo utilizado respecto a seguridad.	• Observación directa • • Tests del cliente • Documentos bibliográficos
		Particularidades del Cliente de Correo Electrónico	13. Existe algún tipo de control de acceso. 14. Prescinde el uso de plug-ins para aumentar las capacidades criptográficas 15. Permanecen los mensajes siempre en servidor evitando el contagio de virus. 16. Utiliza los Protocolos establecidos como estándares (POP3, SMTP)	• Observación directa • Observación directa • Observación directa • Observación directa
		Criptoanálisis	17. Resistencia al criptoanálisis diferencial 18. Resistencia al criptoanálisis lineal	• Observación directa • Observación directa

Tabla # 3.2 Operacionalización de variables – Variable Dependiente

3.4 POBLACION Y MUESTRA

La población es el conjunto de todos los elementos a ser evaluados y en la presente investigación la conforman los Clientes de Correo existentes en el mundo informático, esto incluye a software propietario así como de software libre. Se ha logrado recabar aproximadamente 52 Clientes de Correo a través de Revistas especializadas y sitios que encabezan los primeros lugares de descarga de software especializado de correo electrónico.

De esta población se seleccionó una *muestra no probabilística* basada en 2 criterios de selección:

- Criterio de selección de Clientes de Correo sugeridas por Revistas Especializadas
- Encuesta realizada a distintos tipos de usuarios en nuestro medio

Criterio de selección de Clientes de Correo por Revistas especializadas

CLIENTE DE CORREO	SELECCIÓN DEL EDITOR (25%)	OPINON DEL EDITOR (25%)	OPINIÓN DE MIEMBROS (50%)	SELECCIÓN PROMEDIO
Eudora 6.x	No	●●●●○	●●●●○	✓
Microsoft Outlook 2003	Si	●●●●●	●●○○○	✓
Mailblocks Extended	Si	●●●●○	-	
Mail.com Business	No	●●●○○	●●●○○	
OddpostLotus Notes	Si	●●●●○	-	
Lotus Notes 6	No	-	●●●●○	
Pegasus Mail 4.x	No	●●●○○	●●●●◙	✓

Tabla # 3.3 Criterio de Selección de Clientes de correo – PC Megazine

Encuesta realizada a distintos tipos de usuarios en nuestro medio

El cuestionario se aplicó a un grupo de 56 encuestados, los cuales desempeñaban distintos funciones:

- Docentes – ESPOCH

- Estudiantes – ESPOCH
- Secretarias – Empresa Privada
- Gerentes – Empresa Privada
- Aficionados a Internet – Particulares
- Otros - Particulares

Los resultados obtenidos fueron los siguientes:

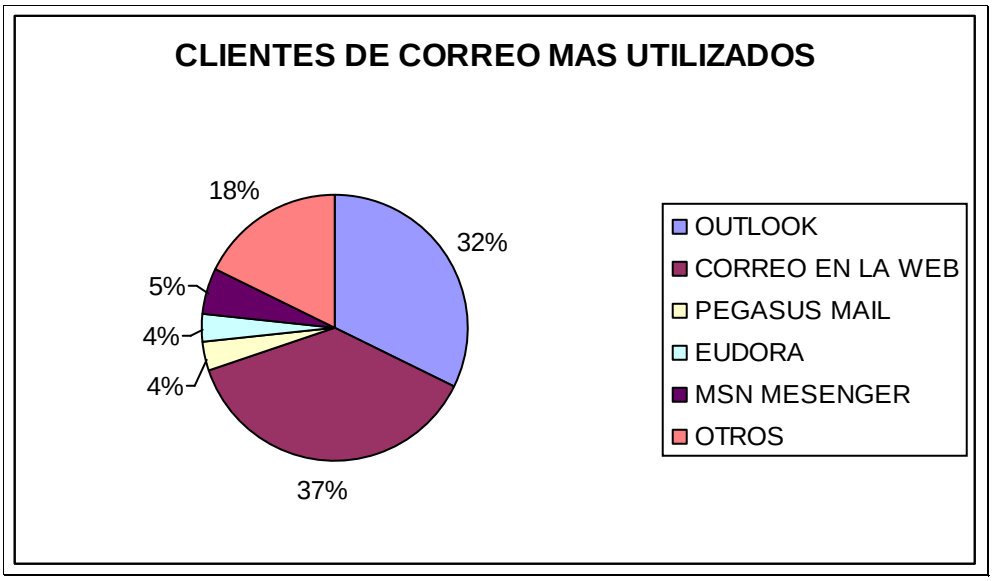


Figura # 3.1 Resultados de encuesta de Clientes de Correo más utilizados

Basándose en los dos criterios de selección antes expuestos se escoge tres administradores de correo apropiados y convenientes para los fines de la investigación y son los siguientes:

- Microsoft Outlook 2003
- Pagasus Mail 4.x
- Eudora 6.x

3.5 PROCEDIMIENTOS GENERALES

Se ha procedido a detallar los métodos utlizados en la presente investigación:

- Investigación de campo

  METODO: Comparativo – Cuasiexperimental

  TECNICAS: Tests – Observación

  INSTRUMENTOS: Guía de Observación

  METODO: Desarrollo de Prototipos

  TECNICAS: Lenguaje UML

  INSTRUMENTOS: Lenguaje Delphi

3.6 INSTRUMENTOS DE LA INVESTIGACION

De acuerdo a la naturaleza de la investigación, los instrumentos más apropiados para la recolección de datos fueron la observación y los tests, los mismos que se aplicaron a los Administradores de Correo seleccionados de acuerdo al criterio ya mencionado en el item 3.2. Se utilizó para ciertos casos la observación directa para comparar a los Administradores de Correo en relación con el Software propuesto por el Investigador y así poder determinar los grados de seguridad del Prototipo propuesto como objetivo de la investigación.

Para realizar los tests se instalaron tres Clientes de Correo en un solo computador a más del software propuesto y se ejecutaban de acuerdo al tipo de prueba que se deseaba probar, comparando así la pertinencia o no de ciertos índices planteados en la operacionalización de las variables.

3.7 VALIDACION DE LOS INSTRUMENTOS

La validez de los instrumentos depende del grado en que se mide el dominio específico de las variables que intervienen en la investigación. De tal forma que para determinar la validez se los instrumentos utilizados se basó en la forma como lo hacen las revistas especializadas (como PC-MEGAZINE) para realizar comparaciones entre Software de Productos de todo tipo, utilizando para esto Pruebas exhaustivas y observaciones directas para seleccionar los mejores productos de Software.

CAPITULO IV

ANALISIS E INTEPRETACION DE RESULTADOS

4.1 PROCESAMIENTO DE LA INFORMACION

Se realizó un análisis tomando en cuenta cada uno de los indicadores de las variables dependiente e independiente y a su vez se consideró cada uno de los índices que conforman cada indicador. Para cuantificar cada uno de los indicadores se utilizó una media ponderada de sus respectivos índices de la siguiente manera:

Indicador 1

Número	Indice	Peso	Calificación
1	Existe algún tipo de generación de clave.	20%	No
2	Se evita la repetición de las claves de sesión.	30%	No
3	Grado de seguridad para evitar que el agresor conozca la forma de distribuir la clave.	30%	Mediana
4	Forma de variabilidad para producir la clave.	20%	Aleatoria
	Total:	**100%**	**55%**

Para la cuantificación de cada índice se utilizó ciertas alternativas o escalas que van de uno a cuatro niveles de acuerdo a aplicabilidad de cada ámbito del índice, como se muestra en la tabla:

1	SI	ALTA	SIEMPRE	TOTALMENTE

2		MEDIANAMEN	FRECUENTE	BASTANTE
3		BAJA	A VECES	POCO
4	NO	MUY BAJA	NUNCA	NADA

Se asignó pesos a cada uno de los índices que conforman un indicador, resultando de esta manera una calificación total por cada Cliente de Correo evaluado. Se calcula luego porcentaje promedio de los tres Clientes de Correo seleccionados, para comparar con el porcentaje individual de la *Propuesta* de la Investigación. Posteriormente para cuantificar las variables dependientes e independientes, se procede a calcular la media ponderada de sus respectivos Indicadores, fijando ponderaciones repartidas equitativamente de porcentaje total por cada una de las variables.

Entonces para calcular el valor de una variable se la realizó de la siguiente manera:

$$Variable = \sum_{i=1}^{n} Peso_i \; Indicador_i$$

Para propósitos de comparación se calculó las medias ponderadas de los indicadores tanto de la variable independiente como de la variable independiente para así determinar la variabilidad entre la Propuesta y otros Clientes de Correo.

4.1.1 RESUMEN DE LAS PRUEBAS DE CLIENTES DE CORREO PARA INDICADORES DE LA VARIABLE INDEPENDIENTE

VARIABLE INDEPENDIENTE: Método alternativo de encriptación para la transmisión de información de un Administrador de Correo Electrónico

INDICADOR 1: Generación de la clave.

	Administrador de Correo			
Índices	Outlook	Pegasus Mail	Eudora	*Propuesta*
1. Existe algún tipo de generación de clave.	No	Si	No	Si
2. Se evita la repetición de las claves de sesión.	No	Si	No	Si
3. Grado de seguridad para evitar que el agresor	Mediana	Alta	Mediana	Alta

conozca la forma de distribuir la clave.				
4. Forma de variabilidad para producir la clave.	Aleatoria	Aleatoria	Aleatoria	Permanen
Totales	35%	85%	35%	100%
Promedio	52%			100%

Tabla # 4.1 Analisis de resultados, variable independiente: Indicador 1

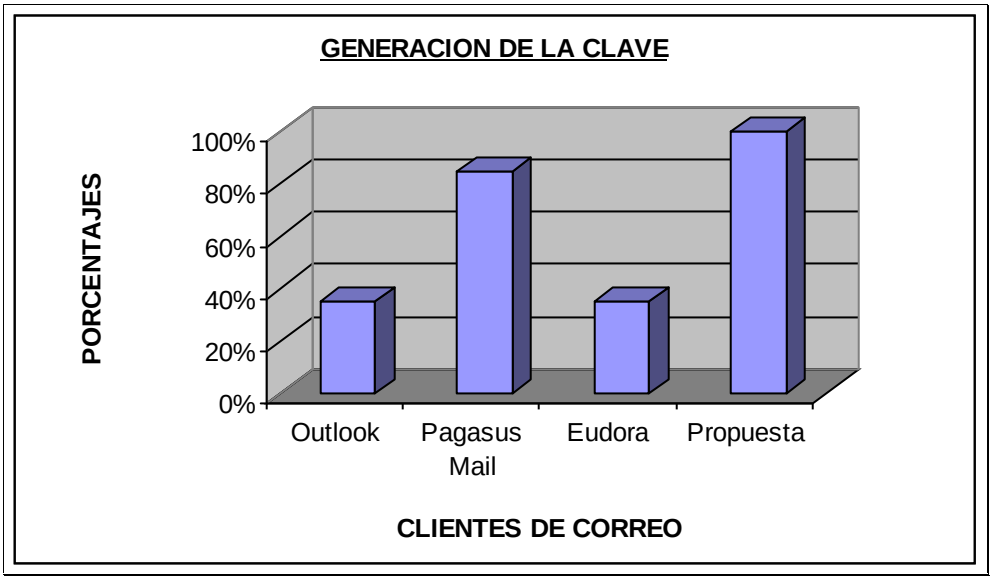


Figura # 4.1 Diagrama de Barras, variable independiente: Indicador 1

Interpretación:

De las pruebas realizadas a los Clientes de Correo se desprende que solo Pegasus Mail genera algún tipo de clave, en base a la solicitud de ingreso de un password, por parte del usuario. Tanto Outlook como Eudora no generan claves por si mismos, a menos que se utilice algún tipo de Servidor de claves o Certificadora de firmas digitales. Eudora y la *Propuesta* de igual manera evitan la repetición de claves de sesión (viaja escondida a través del canal, y se usa una sola vez para el cifrado de un mensaje), para poder así evadir la captura de las mismas por parte de los criptoanalistas. En el índice relacionado a la distribución de claves, sigue liderando Eudora así como la *Propuesta*, ya que los otros Clientes de Correo para poder enviar un mensaje encriptado se necesita que una clave pública viaje o se distribuya por un canal inseguro, cosa que se expone al riesgo de ser capturada, analizada y descubierta. Finalmente en la forma de variar la clave en la *Propuesta* es totalmente permanente por cada segundo que se cree un nuevo correo electrónico a diferencia de los otros Clientes que si utilizarían alguna infraestructura de clave pública se

generaría una clave aleatoria, la cual se puede volverse a repetir. Se concluye por ende que La *Propuesta* posee mejores prestaciones que los otros clientes al generar la clave.

VARIABLE INDEPENDIENTE: Método alternativo de encriptación para la transmisión de información de un Administrador de Correo Electrónico

INDICADOR 2 Encubrimiento de la clave.

	Administrador de Correo			
Índices	Outlook	Pegasus Mail	Eudora	*Propuesta*
5. Existencia de algún tipo de difusión en la clave generada.	No	Si	No	Si
6. Existencia de algún tipo de confusión en la clave generada.	No	Si	No	Si
Totales	0%	100%	0%	100%
Promedio	33%			100%

Tabla # 4.2 Analisis de resultados, variable independiente: Indicador 2

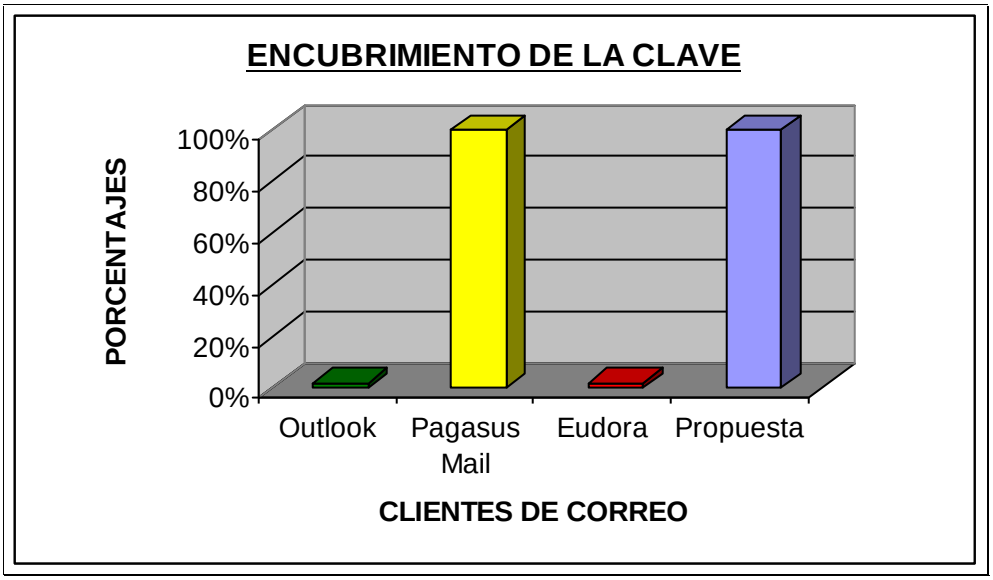


Figura # 4.2 Diagrama de Barras, variable independiente: Indicador 2

Interpretación:

A excepción de Pegasus Mail y la Propuesta los Clientes de Correo no se encargan de encubrir la clave generada ya que si utilizaran Infraestructura de clave pública, para generar una clave, esta se lo haría en forma aleatoria y por ende no se escondería la clave. Hay que tomar también en cuenta que Pegasus Mail utiliza algún tipo de confusión y difusión en la clave, pero se asume que la clave

viaja adjunto al mensaje y encriptada, por lo que esto implica que se pueda analizar de clave mediante algún mecanismo de criptoanálisis. En el gráfico se puede observar que el promedio de los otros clientes de correo es menor en relación a la propuesta de la investigación.

VARIABLE INDEPENDIENTE: Método alternativo de encriptación para la transmisión de información de un Administrador de Correo Electrónico

INDICADOR 3 Características de la encriptación.

	Administrador de Correo			
Índices	Outlook	Pegasus Mail	Eudora	*Propuesta*
7. Se encriptan los mensajes de correo sin interactuar constantemente el usuario	En cierto grado	En cierto grado	En cierto grado	Siempre
8. Velocidad de encriptación en relación a otros procesos de encriptación asimétricos	Mediana	Alta	Mediana	Alta
Totales	67%	83%	67%	100%
Promedio	72%			100%

Tabla # 4.3 Análisis de resultados, variable independiente: Indicador 3

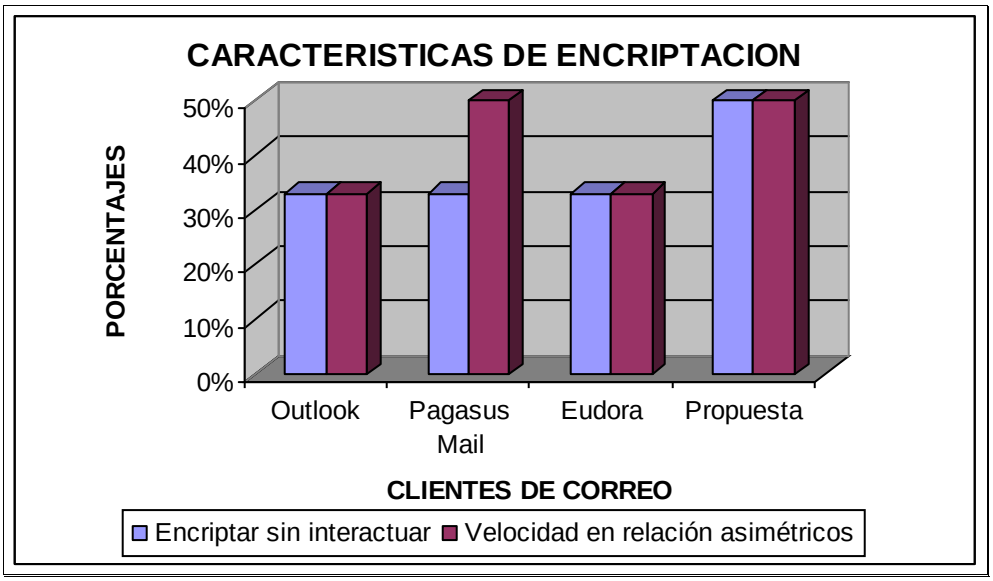


Figura # 4.3 Diagrama de Barras variable independiente: Indicador 3

Interpretación:

Típicamente se puede notar que los Clientes de Correo necesitan interactuar en cierta medida con el usuario, para indicarle que se necesita realizar un proceso de encriptación ya sea mediante una Infraestructura de clave pública o mediante el mecanismo de clave privada (Pegasus Mail). La *Propuesta* de Cliente de Correo, siempre ejecuta el proceso de encriptación por defecto. Por el

contrario la *Propuesta* interactúa con el Cliente de Correo para que sin el caso que desee enviar mensajes pero sin encriptar.

El índice la velocidad de encriptación en relación a otros procesos de encriptación asimétricos queda sujeta básicamente al tipo de algoritmo utilizado ya que a grandes rasgos y en general se puede afirmar que en clave privada se consigue mayores velocidades que la clave pública y de paso que la longitud de las claves que se utilizan son más cortas. Por esa razón La *Propuesta* y Pegasus Mail que utilizan cifrado de llave privada consiguen mayores velocidades de encriptación en relación a los otros administradores de correo electrónico.

VARIABLE INDEPENDIENTE: Método alternativo de encriptación para la transmisión de información de un Administrador de Correo Electrónico

INDICADOR 4 Particularidades del Cliente de Correo electrónico.

	Administrador de Correo			
Índices	Outlook	Pegasus Mail	Eudora	*Propuesta*
9. Existe un método embebido de encriptación en el cliente de correo.	No	Si	No	Si
10. Permanecen los mensajes siempre en servidor evitando el contagio de virus.	A veces	A veces	A veces	Siempre
11. Admite libertad de escoger encriptación o no por parte del usuario.	Si	Si	Si	Si
12. Nivel de transparencia para el usuario del proceso de encriptación.	Mediana	Mediana	Mediana	Alta
Totales	43%	73%	43%	100%
Promedio	53%			100%

Tabla # 4.4 Análisis de resultados, variable independiente: Indicador 4

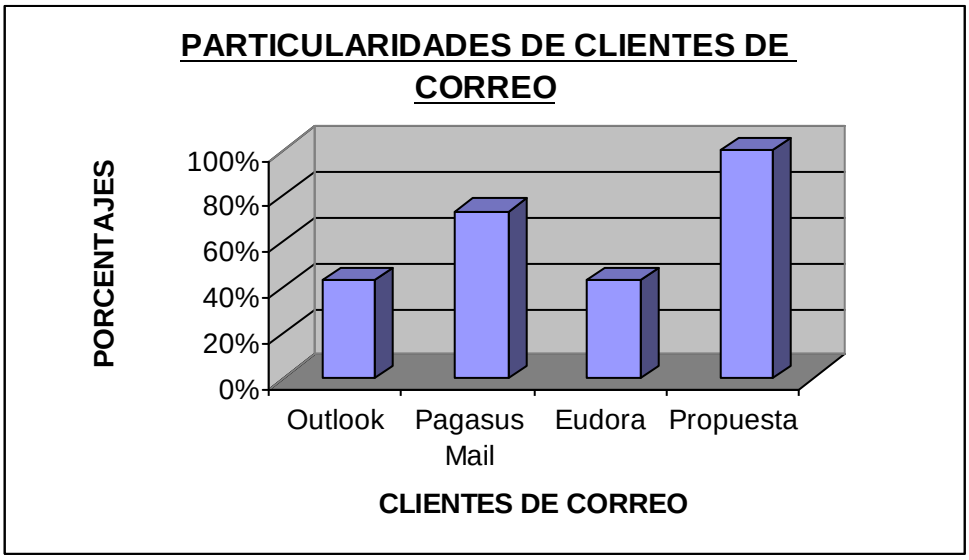


Figura # 4.4 Diagrama de Barras, variable independiente: Indicador 4

Interpretación:

Considerando que las particularidades de los clientes de correo son relacionadas al método de encriptación se puede interpretar en el gráfico que sólo Pegaus Mail y la *Propuesta* incluyen un método embebido de encriptación, cosa que no sucede en el resto de clientes de correo. A esto se suma el índice que indica la permanencia de los mensajes de correo en el servidor, en la que solo la *Propuesta* baja una imagen al Cliente de Correo para que se pueda manipular dicha imagen y no se altere los mensajes mientras permanecen seguros en el Servidor de Correo. Por lo general los clientes de correo, bajan el mensaje del Servidor y lo eliminan; a menos que especifiquen lo contrario.

Todos lo clientes evaluados permiten la libertad de escoger o no encriptación por parte del usuario. Finalmente con respecto al índice que indica el nivel de transparencia para el usuario en el proceso de encriptación, solo la *Propuesta* posee una alta transparencia debido a que cuando envió un mensaje de correo electrónico, automáticamente lo encripta sin interactuar con el usuario, mientras que en los otros clientes de correo siempre tiene que haber un cierto grado de interactividad con el usuario, cosa que no pasa por desapercibido por el usuario. Se concluye manifestando que Pagasus

Mail y la *Propuesta* poseen la más alta puntuación en lo que se refiera a las particularidades de los clientes de correo electrónico.

4.1.2 RESUMEN DE LAS PRUEBAS DE CLIENTES DE CORREO PARA INDICADORES DE LA VARIABLE DEPENDIENTE

VARIABLE DEPENDIENTE: Seguridad en la transmisión y recepción de mensajes

INDICADOR 1: Confidencialidad.

	Administrador de Correo			
Índices	Outlook	Pegasus Mail	Eudora	*Propuesta*
1. Se utiliza cifrado de mensajes	Si	Si	Si	Si
2. Se garantiza el acceso a la información solo al usuario receptor sin utilizar PKI	No	Si	No	Si
3. Se evita la revelación de contenido utilizando otros administradores de correo..	Si	Si	Si	Si
Totales	70%	100%	70%	100%
Promedio	80%			100%

Tabla # 4.5 Análisis de resultados, variable dependiente: Indicador 1

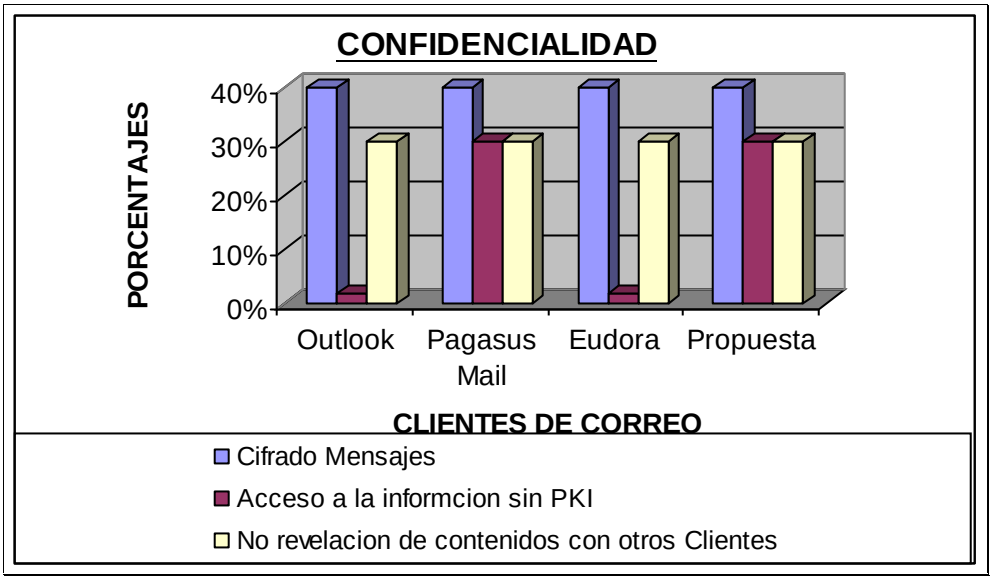


Figura # 4.5 Diagrama de Barras, variable dependiente: Indicador 1

Interpretación:

De los resultados obtenidos se establece que tanto Pegasus Mail como la *Propuesta* tienen total confidencialidad, pero tomando en cuenta que no se utiliza Infraestructura de clave pública, queriendo entenderse que si se puede evitar de alguna manera, distribuir la clave mucho mejor será nuestro sistema de seguridad, no desmereciendo que PKI también goza de cierto grado de seguridad en sus aplicaciones.

VARIABLE DEPENDIENTE: Seguridad en la transmisión y recepción de mensajes

INDICADOR 2: Gestión de claves

	Administrador de Correo			
Índices	Outlook	Pegasus Mail	Eudora	*Propuesta*
4. Tamaño de la clave de al menos 128 bits	Si	No	Si	Si
5. Se evita la repetición de las claves de sesión	No	Si	No	Si
6. Riesgo de evitar que el agresor conozca la forma de distribuir la clave	Mediana	Alto	Mediana	Alto
7. Se genera la clave diferente instantáneamente	Con PKI	Depende	Con PKI	Siempre
8. Existencia de algún tipo de difusión y confusión en la clave generada.	No	Si	No	Si
Totales	43%	66%	43%	100%
Promedio	53%			100%

Tabla # 4.6 Análisis de resultados, variable dependiente: Indicador 2

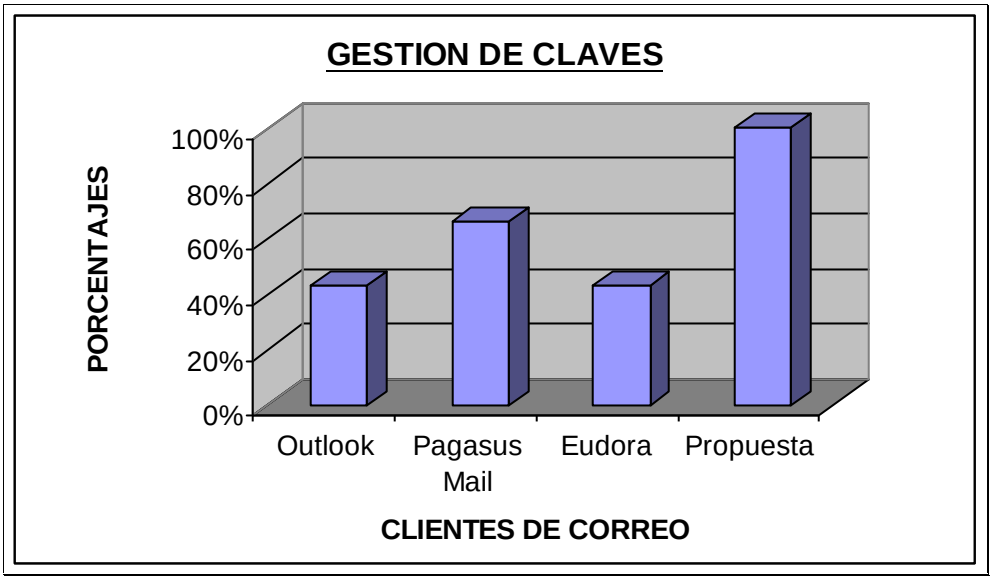


Figura # 4.6 Diagrama de Barras, variable dependiente: Indicador 2

Interpretación:

La solidez de cualquier sistema de cifrado descansa en la técnica de generar, distribuir y esconder la clave y ésta debe estar protegida del acceso a otras partes. Motivo por el cual se denota en los resultados que el Cliente de Correo *Propuesto* evita totalmente la repetición de una clave, el riesgo de conocer su forma de distribuirla e incorpora mecanismos de esconder la clave, en relación con los otros clientes de correo, los cuales no gozan de una total seguridad por su forma de gestionar la claves (típicamente claves públicas). Se considera también el tamaño de las claves ya que si se utiliza más de 128 bits de la longitud de la clave se asegura que sea más complejo en tiempo romper por fuerza bruta la clave.

VARIABLE DEPENDIENTE: Seguridad en la transmisión y recepción de mensajes

INDICADOR 3: Algoritmo de encriptación

	Administrador de Correo			
Índices	Outlook	Pegasus Mail	Eudora	*Propuesta*
9. Utiliza algún algoritmo simétrico.	Con Firmas	Si	Con Firmas	Si
10. Utiliza algún algoritmo asimétrico	Con Firmas	Con firmas	Con Conexio.	No
11. Tiempo de proceso de encriptación.	Llegue PKI	Inmediato	Llegue PKI	Inmediato
12. Tiene popularidad de aceptación el	Bastante	Bastante	Bastante	Completa

algoritmo utilizado respecto a seguridad				
Totales	57%	81%	57%	75%
Promedio	65%			75%

Tabla # 4.7 Análisis de resultados, variable dependiente: Indicador 3

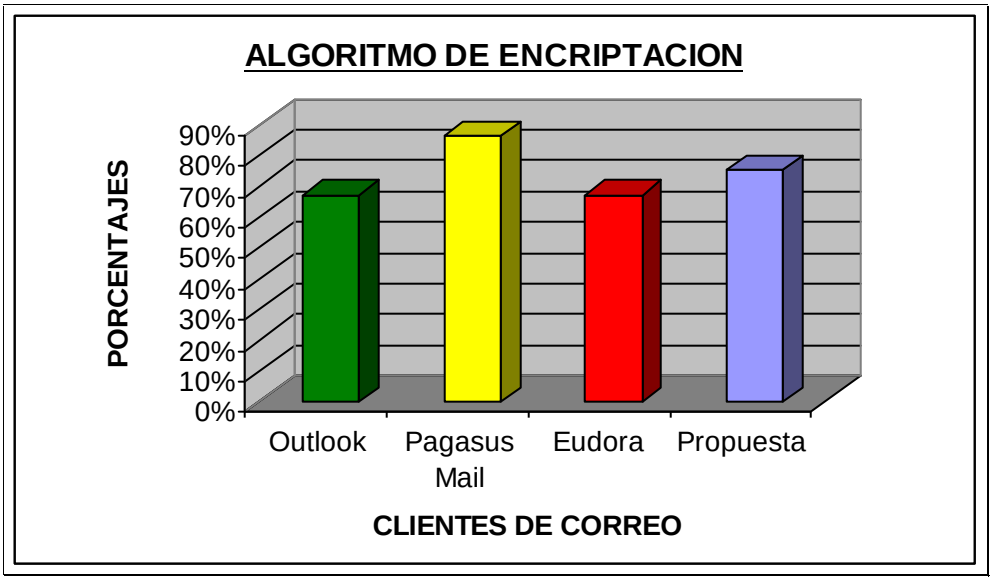


Figura # 4.7 Diagrama de Barras, variable dependiente: Indicador 3

Interpretación:

Conociendo la existencia de dos grandes familias de algoritmos, tanto los de llave pública como los de llave privada, se ha confinado a tomar en cuenta los tipos de algoritmos y además partiendo de que sea un estándar y luego considerando su popularidad en base a opiniones de autores de publicaciones relacionadas a la presente investigación. Se interpreta que casi todos los clientes de correo poseen características de utilización de algoritmos, observándose que la *Propuesta* no utiliza algoritmo de llave pública por las razones anteriormente expuestas.

VARIABLE DEPENDIENTE: Seguridad en la transmisión y recepción de mensajes

INDICADOR 4: Particularidades del Cliente de Correo Electrónico

	Administrador de Correo			
Índices	Outlook	Pegasus Mail	Eudora	*Propuesta*
13. Existe control de acceso al Cliente de Correo	No	No	No	Si

14. Prescinde el uso de plug-ins para aumentar las capacidades criptográficas	Si	Si	No	Si
15. Permanecen los mensajes siempre en servidor evitando el contagio de virus.	A veces	A veces	A veces	Siempre
16. Utiliza Protocolos estándares (POP3, SMTP) para encriptar	Si	Si	No	Si
Totales	63%	63%	13%	100%
Promedio	46%			100%

Tabla # 4.8 Análisis de resultados, variable dependiente: Indicador 4

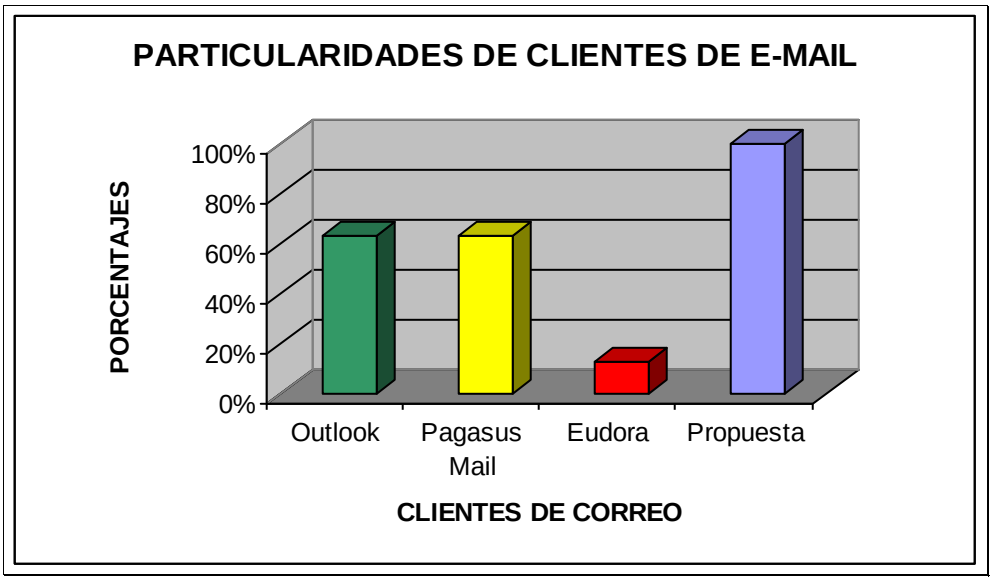


Figura # 4.8 Diagrama de Barras, variable dependiente: Indicador 4

Interpretación:

Normalmente los Clientes de Correo necesitan de aditamentos para aumentar ciertas capacidades tales como las utilidades criptográficas, siendo esta la característica fundamental de la Propuesta. Otra característica típica de los Clientes de Correo es que al conectarse al Servidor de correo se baja automáticamente todos los mensajes hacia al cliente, quedando expuestos a cualquier tipo de amenaza, esto se evita en la *Propuesta* ya que solo se baja una imagen del mensaje y así poder revisarlo tranquilamente, evitando el contagio de algún tipo de virus (por permanecer en el servidor). Los otros clientes de correo por defecto se bajan los correos a menos que por conveniencia lo configuren de esa manera. Finalmente se debe recalcar que la Propuesta de Correo encripta los mensajes de correo electrónico, utilizando los estándares de transmisión de correo (SMTP, POP3), característica Pegasus Mail y la propuesta incorpora, ya que muchos software de correo implementan la característica de protección de la información con otros protocolos seguros

como S/MIME o SSL. Se concluye que la *Propuesta* de Correo posee ciertas particularidades que los hacen mas seguro frente a los otros Clientes de Correo.

VARIABLE DEPENDIENTE: Seguridad en la transmisión y recepción de mensajes

INDICADOR 5: Criptoanálisis

	Administrador de Correo			
Índices	Outlook	Pegasus Mail	Eudora	*Propuesta*
17. Resistencia al criptoanálisis diferencial	Alta	Mediana	Alta	Alta
18. Resistencia al criptoanálisis lineal	Alta	Mediana	Alta	Alta
Totales	100%	68%	100%	100%
Promedio	90%			100%

Tabla # 4.9 Análisis de resultados, variable dependiente: Indicador 5

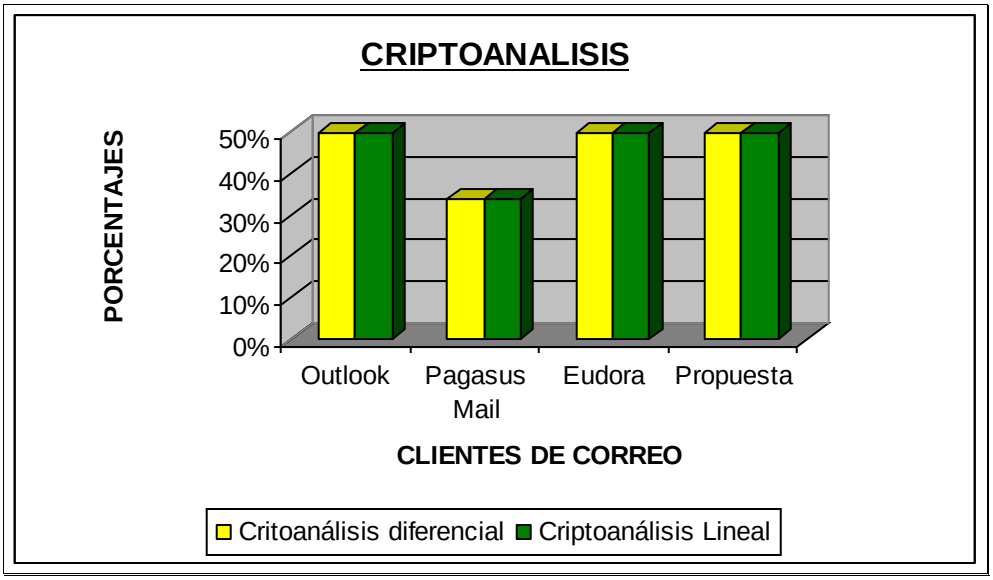


Figura # 4.9 Diagrama de Barras, variable dependiente: Indicador 5

Interpretación:

El Criptoanálisis es el conjunto de técnicas y métodos que se utilizan para descifrar mensajes. Al estar relacionado con los algoritmos utilizados y conociendo que Pegasus Mail utiliza la especificación DES, la cual ha sido rota con ciertas especificaciones, se evalúa con una residencia Mediana, la cual superan los otros Clientes de Correo debido a su implantación de algoritmos resistentes al criptoanálisis diferencial y lineal, como son IDEA, AES, etc.

4.1.3 RESUMEN DE LAS EQUIVALENCIAS DE LOS PESOS PARA INDICADORES DE LA VARIABLE INDEPENDIENTE

Administrador de Correo			**Outlook**	**Pegasus Mail**	**Eudora**	**Propuesta**
INDICADORES	GENERACION DE LA CLAVE	**1** (20%)	0%	20%	0%	20%
		2 (30%)	0%	30%	0%	30%
		3 (30%)	20%	30%	20%	30%
		4 (20%)	15%	15%	15%	20%
		Total (100%)	**35%**	**85%**	**35%**	**100%**
	ENCUBRIMIENTO DE LA CLAVE	**5** (50%)	0%	50%	0%	50%
		6 (50%)	0%	50%	0%	50%
		Total (100%)	**0%**	**100%**	**0%**	**100%**
	CARACTERISTICA DE LA ENCRIPTACION	**7** (50%)	33%	33%	33%	50%
		8 (50%)	33%	50%	33%	50%
		Total (100%)	**67%**	**83%**	**67%**	**100%**
	PARTICULARID	**9**	0%	30%	0%	30%

	ADES DEL CLIENTE DE CORREO ELECTRONICO	(30%)				
		10 (30%)	10%	10%	10%	30%
		11 (20%)	20%	20%	20%	20%
		12 (20%)	13%	13%	13%	20%
		Total (100%)	**43%**	**73%**	**43%**	**100%**

Tabla # 4.10 Resumen de pesos para indicadores de la variable independiente

4.1.4 RESUMEN DE LAS EQUIVALENCIAS DE LOS PESOS PARA INDICADORES DE LA VARIABLE DEPENDIENTE

Administrador de Correo			**Outlook**	**Pegasus Mail**	**Eudroa**	**Propuesta**
INDICADORES	CONFIDENCIALI-DAD	**1** (40%)	40%	40%	40%	40%
		2 (30%)	0%	30%	0%	30%
		3 (30%)	30%	30%	30%	30%
		Total (100%)	70%	100%	70%	100%
	GESTION DE CLAVES	**4** (20%)	20%	0%	20%	20%
		5 (20%)	0%	20%	0%	20%
		6 (20%)	13%	20%	13%	20%
		7 (20%)	10%	13%	10%	20%
		8 (20%)	0%	20%	0%	20%
		Total (100%)	43%	73%	43%	100%
	ALGORITMO DE ENCRIPTACION	**9** (25%)	13%	25%	13%	25%
		10 (25%)	13%	13%	13%	0%
		11 (25%)	13%	25%	13%	25%
		12 (25%)	18%	18%	18%	25%
		Total (100%)	57%	81%	57%	75%

	PARTICULARI-DADES DEL CLIENTE DE CORREO ELECTRONICO	**13** (25%)	0%	0%	0%	25%
		14 (25%)	25%	25%	0%	25%
		15 (25%)	13%	13%	13%	25%
		16 (25%)	25%	25%	0%	25%
		Total (100%)	63%	63%	13%	100%
	CRIPTOANALISIS	**17** (50%)	50%	34%	50%	50%
		18 (50%)	50%	34%	50%	50%
		Total (100%)	100%	68%	100%	100%

Tabla # 4.11 Resumen de pesos para indicadores de la variable dependiente

4.2 ANALISIS DE RESULTADOS

4.2.1 VARIABLE INDEPENDIENTE

Tomando en cuenta que cada indicador tiene su peso, entonces se desglosa cada uno de los promedios de los indicadores.

V. INDEPENDIENTE:	**Método alternativo de encriptación para la transmisión de información de un administrador de correo electrónico**		
CLIENTES DE CORREO		**Otros**	**Propuesta**
INDICADORES	Generación de la clave (25%)	52%	100%
	Encubrimiento de la clave (25%)	33%	100%
	Características de la encriptación (25%)	72%	100%
	Particularidades del Cliente de Correo Electrónico (25%)	53%	100%

Tabla # 4.12 Análisis de resultados, variable independiente: Total Indicadores

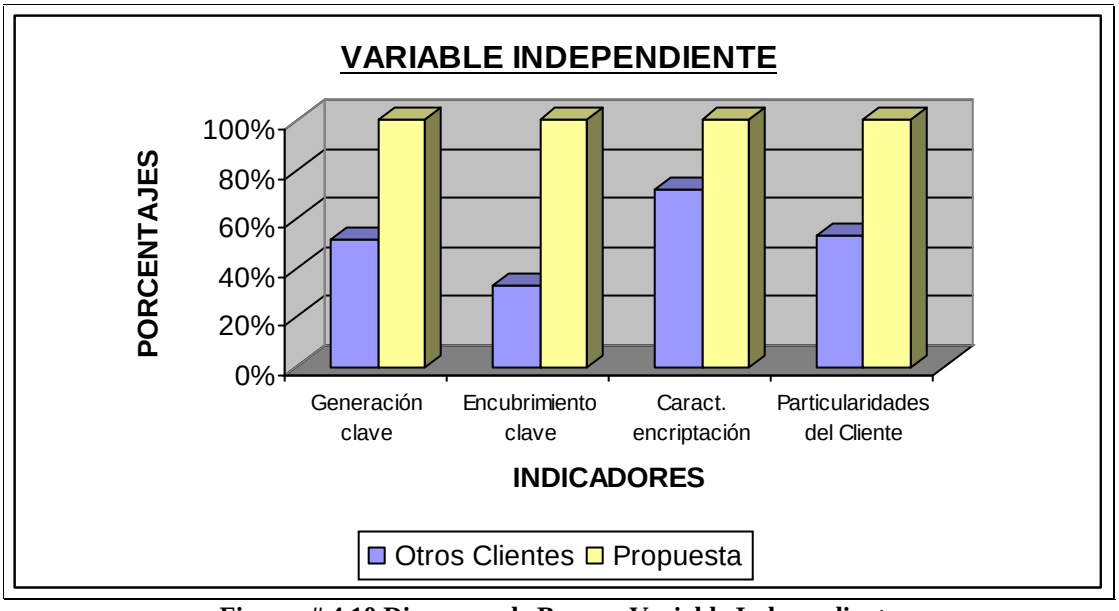


Figura # 4.10 Diagrama de Barras, Variable Independiente

V.I. (Otros) = 0.25(52) + 0.25(33) + 0.25(72) + 0.25(53) = **53%**

V.I (Propuesta) = 0.25(100) + 0.25(100) + 0.25(100) + 0.25(100) = **100%**

Variabilidad = V.I. (Propuesta) – V.I. (Otros) = 100% - 53% = **47%**

Interpretación:

Se concluye que el Método de encriptación para la transmisión de la información de un administrador de correo electrónico es un 47% alternativo en relación a otros Administradores de Correo.

4.2.2 VARIABLE DEPENDIENTE

Tomando en cuenta que cada indicador tiene su peso, entonces se desglosa cada uno de los promedios de los indicadores.

V. DEPENDIENTE:	**Seguridad en la transmisión y recepción de Mensajes**		
CLIENTES DE CORREO		**Otros**	**Propuesta**
INDICADORES	Confidencialidad (20%)	80%	100%
	Gestión de claves (20%)	53%	100%
	Algoritmo de encriptación (20%)	65%	75%
	Particularidades del Cliente de Correo Electrónico (20%)	46%	100%
	Criptoanálisis (20%)	90%	100%

Tabla # 4.13 Análisis de resultados, variable dependiente: Total Indicadores

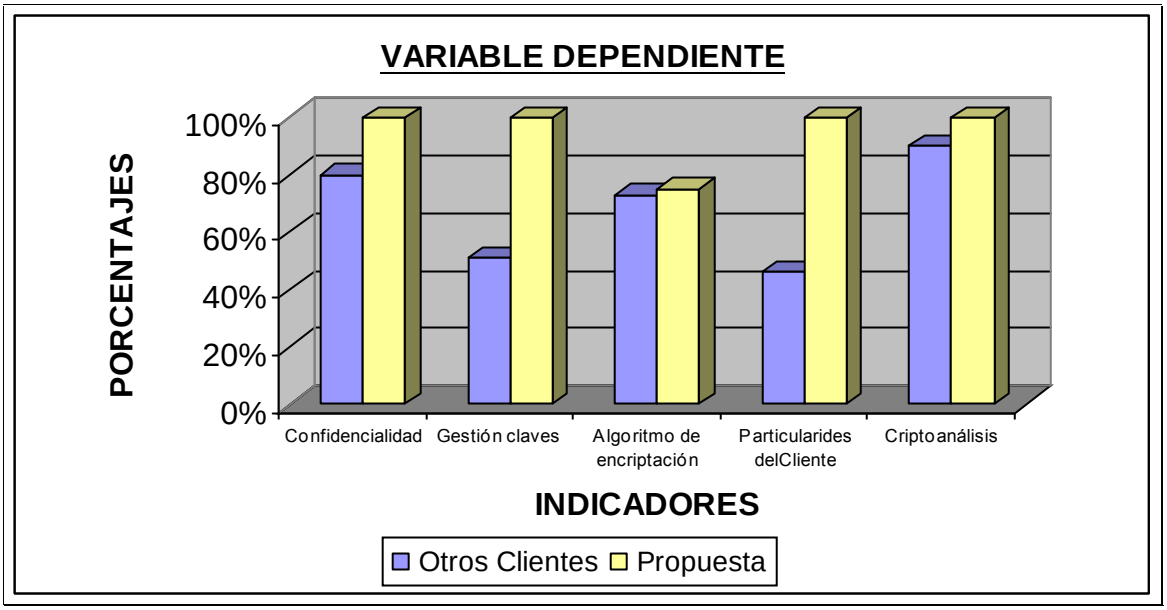


Figura # 4.11 Diagrama de Barras, Variable Dependiente

V.D. (Otros) = 0.2(80) + 0.2(53) + 0.2(65) + 0.2(46) + 0.2(90) = **67%**

V.D (Propuesta) = 0.2(100) + 0.2(100) + 0.2(75) + 0.2(100) + 0.2(100) = **95%**

Variabilidad = V.D. (Propuesta) – V.D. (Otros) = 95% - 68%% = **28%**

Interpretación:

Se concluye que La Seguridad en la transmisión y recepción de mensajes de correo electrónico se fortalecerá en un 28%

4.3 PRUEBA DE LA HIPOTESIS

Para demostrar la hipótesis se estableció la variabilidad o diferencia de cada una de las variables, tal como se indica en la siguiente tabla:

	Otros Clientes de Correo	**Propuesta**	**Diferencia**
Variable Independiente	53%	100%	47%
Variable Dependiente	67%	95%	28%

Tabla # 4.14 Análisis de resultados, Diferencia de las Variables

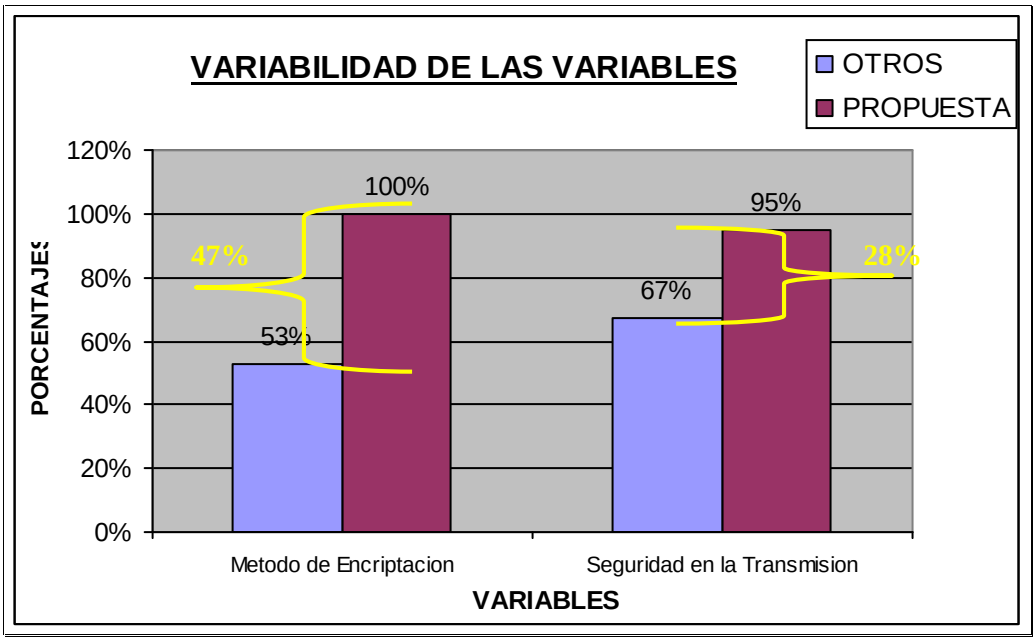


Figura # 4.12 Diagrama de Barras, Diferencia de las Variables

Se demuestra la hipótesis corroborando que La Seguridad en la transmisión y recepción de mensajes de correo electrónico se fortalecerá en un 28% al utilizar el Método al 47% alternativo de encriptación dinámica para la transmisión de información de un Administrador de Correo electrónico.

CAPITULO V

MARCO PROPOSITIVO

5.1 PROPUESTA DEL METODO ALTERNATIVO DE ENCRIPTACION DINAMICA

Para plantear la forma de encriptar la información que se envía y recibe a través del correo electrónico, se consideró que los mensajes que circulan por Internet, que son decenas de millones diariamente, lo hacen por un número indeterminado de computadores y cualquier Administrador podría acceder a la información. Entonces, un usuario común utiliza un Cliente de Correo que por defecto *no incluyen características de encriptación* y si se desea usar los servicios de encriptación se necesita una infraestructura de clave pública, la cual implica obtener un Certificado emitido por una Certificadora, lo cual se hace embarazoso para el usuario.

Además se pensó, que si al utilizar un Cliente de Correo que genere claves aleatorias, los usuarios pueden no ser capaces de recordarlas, más aún si el esquema, es permitirle al usuario elegir su propia contraseña, entramos al riesgo de elegir las mismas claves y en general es más fácil realizar criptoanálisis con mucho texto cifrado con la misma clave. **Por esta razón se pensó en la variabilidad de las claves, provocando a su vez la variabilidad en el criptosistema**.

Tomando en cuenta las consideraciones anteriormente expuestas se propone:

Procedimiento de encriptación en el emisor:

1. Se **analiza** la cabecera del mensaje creado de acuerdo al estándar RFC 822
2. Se **genera** una clave primaria de acuerdo a los parámetros utilizados en la cabecera del mensaje creado
3. Se **encubre** la clave generada mediante la difusión y la confusión
4. Con la **clave encubierta** y el algoritmo **IDEA** se **encripta** el cuerpo del mensaje
5. El resultado (mensaje cifrado) se envía a través del protocolo SMTP.

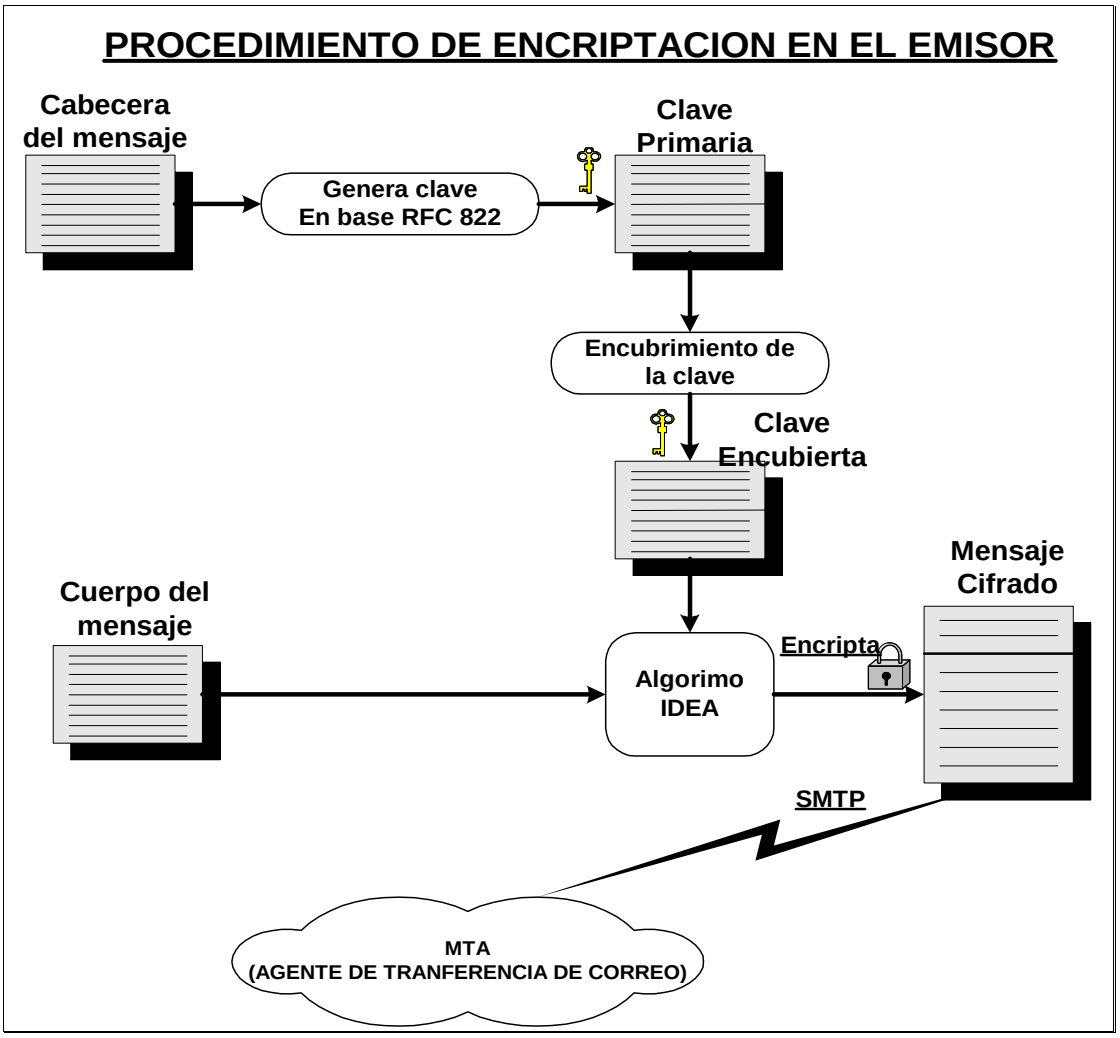


Figura # 5.1 Gráfico del proceso de encriptación en el emisor

Procedimiento de desencriptación en el receptor:

1. Se **recibe** el mensaje cifrado mediante el protocolo POP3
2. Se **analiza** la cabecera del mensaje receptado de acuerdo al estándar RFC 822
3. Se **genera** una clave primaria de acuerdo a los parámetros utilizados en la cabecera del mensaje receptado
4. Se **encubre** la clave generada mediante la difusión y la confusión
5. Con la **clave encubierta** y el algoritmo **IDEA** se **desencripta** el cuerpo del mensaje cifrado
6. El resultado (mensaje original) se muestra al usuario de correo.

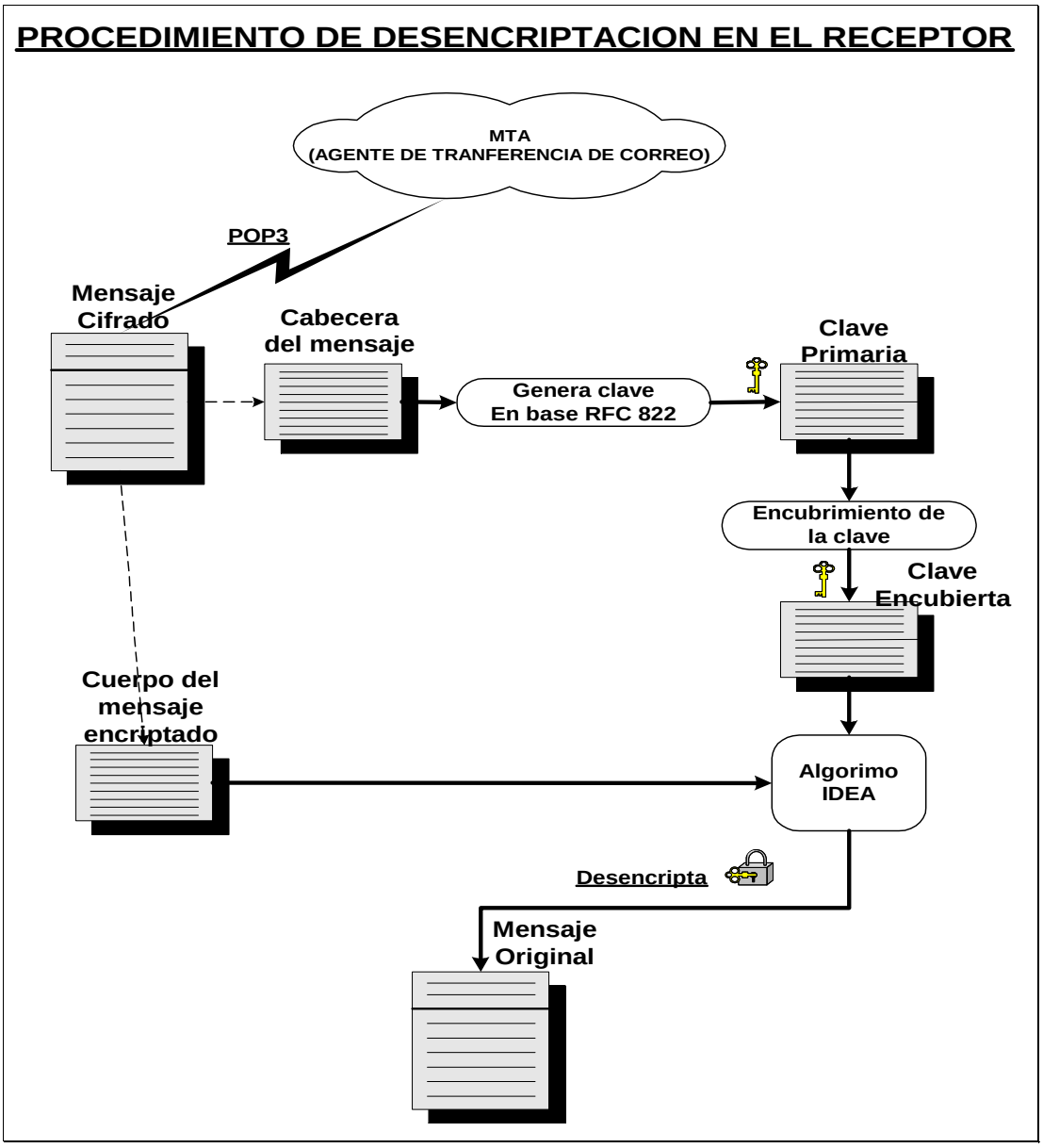


Figura # 5.2 Gráfico del proceso de desencriptación en el receptor

5.2 PARAMETROS DE GENERACION DE LA CLAVE DINAMICA

Para la generación de la clave se ha considerado sujetarse a los estándares relacionados con el manejo de los Agentes de Usuario, es decir el estándar **RFC 822** referente al **Formato y Codificación Básica de Mensajes**, que especifica la sintaxis para los mensajes de texto que son enviados por los usuarios de computadoras en el ámbito del correo electrónico. En este contexto, los mensajes son vistos como encabezado y un contenido. El encabezado contiene información necesaria para permitir la transmisión y entrega del mensaje. El contenido es la información propiamente dicha que se entregará a un destinatario.

De acuerdo a la especificación de mensajes establecida en el estándar se tomó en cuenta los campos de la cabecera que son cambiantes o **dinámicos** de acuerdo a como se genere el correo y se propone los siguientes:

- **Fecha y Hora de envío del mensaje** [**F1]** .- Cambia en segundos, minutos, horas, días, meses y años
- **Remitente [F2]**.- Cada usuario que tenga una cuenta de correo electrónico y genere un mensaje.
- **Destinatario (uno o múltiples, con copia) [F3]**.- Cada usuario al que se le emita un mensaje de correo electrónico.
- **Prioridad [F4]**.- Por el tipo de prioridad que se de al mensaje (alta, baja, normal)
- **Datos adjuntos [F5]**.- Las veces que a un mensaje se le añada un archivo de cualquier tipo que éste sea.
- **Cantidad de caracteres en el asunto (Subject) [F6]**.- La cadena de caracteres que se escriba en el Titulo del mensaje.
- **Cantidad de bits para complementar la clave [F7]**.- Cantidad de datos complementarios para completar el total de bits exigidos por el algoritmo.

5.3 DESCRIPCION DE LA GENERACION DE LA CLAVE DINAMICA

5.3.1 GENERACION DE LA FECHA Y HORA DE ENVIO DEL MENSAJE

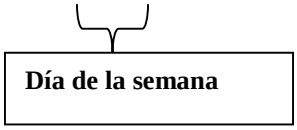
El formato que se genera para el envío del correo es el siguiente:

Date: Mon, 1 Dec 2003 14:52:19 +0100

Entonces subdividimos en partes la fecha del envío:

Día de la semana

Date: Mon, 1 Dec 2003 14:52:19 +0100



Cantidad de dígitos utilizados: **3**

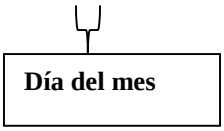
Codificación

Día de la semana	Codificación
Mon	001
Tue	010
Wed	011
Thu	100
Fri	101
Sat	110
Sun	111

Tabla # 5.1 Codificación de la fecha y hora: Día de la semana

Día del mes

Date: Mon, 1 Dec 2003 14:52:19 +0100



Cantidad de dígitos utilizados: **6**

Codificación:

Día del mes	Paridad	Codificación
1	1	100001
2	0	000010
3	1	100011
4	0	000100
5	1	100101
6	0	000110
7	1	100111
8	0	001000
9	1	101001
10	0	001010
11	1	101011
12	0	001100
13	1	101101
14	0	001110
15	1	101111
16	0	010000
17	1	110001
18	0	010010
19	1	110011
20	0	010100
21	1	110101
22	0	010110
23	1	110111
24	0	011000
25	1	111001
26	0	011010
27	1	111011
28	0	011100
29	1	111101
30	0	011110
31	1	111111

Tabla # 5.2 Codificación de la fecha y hora: Día del mes

Mes del año

Date: Mon, 1 Dec 2003 14:52:19 +0100

Cantidad de dígitos utilizados: **5**

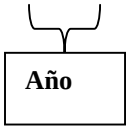
Codificación

Día del mes	Paridad	Codificación
Jan	1	10001
Feb	0	00010
Mar	1	10011
Apr	0	00100
May	1	10101
Jun	0	00110
Jul	1	10111
Aug	0	01000
Sep	1	11001
Oct	0	01010
Nov	1	11011
Dec	0	01100

Tabla # 5.3 Codificación de la fecha y hora: Mes del año

<u>Año de generación</u>

Date: Mon, 1 Dec 2003 14:52:19 +0100



Cantidad de dígitos utilizados: **12**

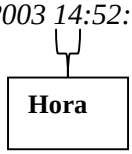
Codificación

Año	Paridad	Codificación
2000	0	011111010000
2001	1	111111010001
2002	0	011111010010
2003	1	111111010011
2004	0	011111010100
2005	1	111111010101
2006	0	011111010110
2007	1	111111010111
2008	0	011111011000

Tabla # 5.4 Codificación de la fecha y hora: Año de generación

Hora de generación

Date: Mon, 1 Dec 2003 14:52:19 +0100



Cantidad de dígitos utilizados: **5**

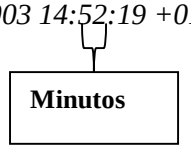
Codificación

Hora	Codificación
01	00001
02	00010
03	00011
04	00100
05	00101
06	00110
07	00111
08	01000
09	01001
10	01010
11	01011
12	01100
13	01101
14	01110
15	01111
16	10000
17	10001
18	10010
19	10011
20	10100
21	10101
22	10110
23	10111
24	11000

Tabla # 5.5 Codificación de la fecha y hora: Hora de generación

Minutos de la hora de generación

Date: Mon, 1 Dec 2003 14:52:19 +0100



Cantidad de dígitos utilizados: **6**

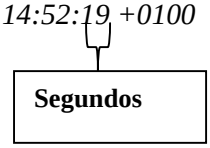
Codificación

Minutos	Codificación
01	000001
02	000010
03	000011
04	000100
05	000101
06	000110
07	000111
08	001000
09	001001
10	001010
11	001011
12	001100
13	001101
14	001110
15	001111
16	010000
17	010001
18	010010
19	010011
20	010100
21	010101
22	010110
23	010111
24	011000
25	011001
26	011010
27	011011
28	011100
29	011101
30	011110
.	.
.	.
.	.
58	111010
59	111011
60	111100

Tabla # 5.6 Codificación de la fecha y hora: Minutos de la hora de generación

Segundos del minuto generado

Date: Mon, 1 Dec 2003 14:52:19 +0100



Cantidad de dígitos utilizados: **6**

Codificación

Minutos	Codificación
01	000001
02	000010
03	000011
04	000100
05	000101
06	000110
07	000111
08	001000
09	001001
10	001010
11	001011
12	001100
13	001101
14	001110
15	001111
16	010000
17	010001
18	010010
19	010011
20	010100
.	.
.	.
.	.
.	.
.	.
58	111010
59	111011
60	111100

Tabla # 5.7 Codificación de la fecha y hora: Segundos del minuto generado

<u>Zona horaria</u>

Date: Mon, 1 Dec 2003 14:52:19 +0100

Zona horaria

Cantidad de dígitos utilizados: **6**

Codificación

Zona horaria	Codificación
UT	000001
GMT	000010
EST	000011
EDT	000100
CST	000101
CDT	000110
MST	000111
MDT	001000
PST	001001
PDT	001010
+1200	001011
+1100	001100
+1000	001101
+0900	001110
+0800	001111
+0700	010000
+0600	010001
+0500	010010
+0400	010011
+0300	010100
+0200	010101
+0100	010110
-1200	010111
-1100	011000
-1000	011001
-0900	011010
-0800	011011
-0700	011100
-0600	011101
-0500	011110
-0400	011111
-0300	100000
-0200	100001
-0100	100010

Tabla # 5.8 Codificación de la fecha y hora: Zona Horaria

TOTAL DE BITS UTILIZADOS **EN FECHA Y HORA DE ENVIO DEL MENSAJE**

[F1] = Día de la semana + Día del mes + Mes del año + Año de generación + Hora de generación + Minutos de la Hora + Segundos del minuto + Zona Horaria

[F1] = 3 + 6 + 5 + 12 + 5 + 6 + 6 + 6 = **49 bits** de la Fecha y hora de envío del mensaje

[F1] = 49 bits

5.3.2 GENERACION DEL REMITENTE DEL MENSAJE

El formato que se genera para el envío del correo es el siguiente:

From: "Goyes Jose Luis" <goyesj@produbanco.com>

Entonces subdividimos en partes el remitente del mensaje:

Número de caracteres del nombre de usuario

From: "Goyes Jose Luis" <goyesj@produbanco.com>

Usuario de correo

Cantidad de dígitos utilizados: **5**

Codificamos de acuerdo a la cantidad de caracteres que tenga el nombre de usuario

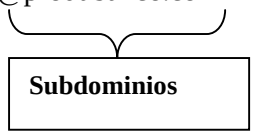
Codificación

Número de Caracteres	Codificación
01	00001
02	00010
03	00011
04	00100
05	00101
06	00110
07	00111
08	01000
09	01001
10	01010
11	01011
12	01100
.	.
.	.
.	.
.	.
31	11111

Tabla # 5.9 Codificación del Remitente: Número de caracteres de usuario

Número de subdominios de la dirección de dominio

From: "Goyes Jose Luis" <goyesj@produbanco.com>



Cantidad de dígitos utilizados: **3**

Codificamos de acuerdo a la cantidad de subdominios que tenga el nombre de dominio

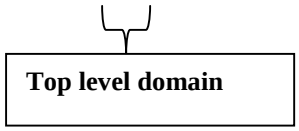
Codificación

Número de subdominios	Codificación
1	001
2	010
3	011
4	100
5	101
6	110
7	111

Tabla # 5.10 Codificación del Remitente: Número de subdominios

Dominio de más alto nivel de la dirección de correo

From: "Goyes Jose Luis" <goyesj@produbanco.com>



Codificamos de acuerdo al estándar **ISO-3166-1** en concordancia de los respectivos dominios.

Cantidad de dígitos utilizados: **10**

Codificación de Dominios especiales

Dominios especiales	Codificación	Descripción
gov	1111101001	Organizaciones Gubernamentales
edu	1111101010	Organizaciones Educacionales
mil	1111101011	Organizaciones Militares
com	1111101100	Organizaciones Comerciales
org	1111101101	Organizaciones no lucrativas
net	1111101110	Organizaciones de Redes
int	1111101111	Organizaciones Internacionales
uucp	1111110000	Red UUCP
bitnet	1111110000	Red BITNET
otros	1111111111	Cualquier otro dominio no contemplado

Tabla # 5.11 Codificación del Remitente: Dominios Especiales

Codificación de Dominios geográficos

Dominio	Codificación	País	Dominio	Codificación	País
Af	0000000100	Afghanistan	cl	0010011000	Chile
Al	0000001000	Albania	cn	0010011100	China, mainland
Dz	0000001100	Algeria	cx	0010100010	Christmas Island
As	0000010000	American Samoa	cc	0010100110	Cocos Islands
Ad	0000010100	Andorra	co	0010101010	Colombia
Ao	0000011000	Angola	km	0010101110	Comoros
Ai	1010010100	Anguilla	cg	0010110010	Congo, Republic
Aq	0000001010	Antarctica	cd	0010110100	Congo, Democratic
Ag	0000011100	Antigua and Barbud.	ck	0010111000	Cook Islands
Ar	0000100000	Argentina	cr	0010111100	Costa Rica
Am	0000110011	Armenia	ci	0110000000	Côte d'Ivoire
aw	1000010101	Araba	hr	0010111111	Croatia
au	0000100100	Australia	cu	0011000000	Cuba
at	0000101000	Austria	cy	0011000100	Cyprus
az	0000011111	Azerbaijan	cz	0011001011	Czech Republic
bs	0000101100	Bahamas	dk	0011010000	Denmark
bh	0000110000	Bahrain	dj	0100000110	Djibouti
bd	0000110010	Bangladesh	dm	0011010100	Dominica
bb	0000110100	Barbados	do	0011010110	Dominican Republic
by	0001110000	Belarus	ec	0011011010	Ecuador
be	0000111000	Belgium	eg	1100110010	Egypt
bz	0001010100	Belize	sv	0011011110	El Salvador
bj	0011001100	Benin	gq	0011100010	Equatorial Guinea
bm	0000111100	Bermuda	er	0011101000	Eritrea
bt	0001000000	Bhutan	ee	0011101001	Estonia
bo	0001000100	Bolivia	et	0011100111	Etiopía
ba	0001000110	Bosnia and Resegó.	fk	0011101110	Falkland Islands
bw	0001001000	Botswana	fo	0011101010	Faroe Islands
bv	0001001010	Bouvet Island	fj	0011110010	Fiji
br	0001001100	Brazil	fi	0011110110	Finland
io	0001011100	British Indian Ocean	fr	0011111010	France
bn	0001100000	Brunei Darussalam	gf	0011111110	French Guiana
bg	0001100100	Bulgaria	pf	0100000010	French Polynesia
bf	1101010110	Burkina Faso	tf	0100000100	French Southern
bi	001101100	Burundi	ga	0100001010	Gabon
kh	0001110100	Cambodia	gm	0100001110	Gambia
cm	0001111000	Cameroon	ge	0100001100	Georgia
ca	0001111100	Canada	de	0100010100	Germany
cv	0010000100	Cape Verde	gh	0100100000	Ghana
ky	0010001000	Cayman Islands	gi	0100100100	Gibraltar
cf	0010001100	Central African	gr	0100101100	Greece
td	0010010100	Chad	gl	0100110000	Greenland

Codificación de Dominios geográficos (continuación ……)

Dominio	Codificación	País	Dominio	Codificación	País
gd	0100110100	Grenada	mg	0111000010	Madagascar
gp	0100111000	Guadeloupe	mw	0111000110	Malawi
gu	0100111100	Guam	my	0111001010	Malaysia
gt	0101000000	Guatemala	mv	0111001110	Maldives
gn	0101000100	Guinea	Ml	0111010010	Mali
gw	1001110000	Guinea-Bissau	Mt	0111010110	Malta
gy	0101001000	Guyana	Mh	1001001000	Marshall Islands
ht	0101001100	Haiti	Mq	0111011010	Martinique
hm	0101001110	Heard and McDonaldl	Mr	0111011110	Mauritania
hn	0101010100	Honduras	Mu	0111100000	Mauritius
hk	0101011000	Hong Kong	Yt	0010101111	Mayotte
hu	0101011100	Hungary	Mx	0111100100	Mexico
is	0101100000	Iceland	Fm	1001000111	Micronesia, Fed
in	0101100100	India	Md	0111110010	Moldova, Republic
id	0101101000	Indonesia	Mc	0111101100	Monaco
ir	0101101100	Iran, Islamic Republic	Mn	0111110000	Mongolia
iq	0101110000	Iraq	Ms	0111110100	Montserrat
ie	0101110100	Ireland, Republic of	Ma	0111111000	Morocco
im	1101000001	Isle of Man	Mz	0111111100	Mozambique
il	0101111000	Israel	Mm	0001101000	Myanmar
it	0101111100	Italy	Na	1000000100	Namibia
jm	0110000100	Jamaica	Nr	1000001000	Nauru
jp	0110001000	Japan	Np	1000001100	Nepal
jo	0110010000	Jordan	Nl	1000010000	Netherlands
kz	0110001110	Kazakhstan	An	1000010010	Netherlands Antill.
ke	0110010100	Kenya	Nc	1000011100	New Caledonia
ki	0100101000	Kiribati	Nz	1000101010	New Zealand
kp	0110011000	Korea, Democratic	Ni	1000101110	Nicaragua
kr	0110011010	Korea, Republic of	Ne	1000110010	Níger
kw	0110011110	Kuwait	Ng	1000110110	Nigeria
kg	0110100001	Kyrgyzstan	Un	1000111010	Niue
la	0110100010	Lao People's Democra.	Nf	1000111110	Norfolk Island
lv	0110101100	Latvia	Mp	1001000100	Northern Mariana I.
lb	0110100110	Lebanon	No	1001000010	Norway
ls	0110101010	Lesotho	Om	1000000000	Oman
lr	0110101110	Liberia	Pk	1001001010	Pakistan
ly	0110110010	Libyan Arab Jamahiriya	Pw	1001001001	Palau
li	0110110110	Liechtenstein	Ps	0100010011	Palestinian Territo.
lt	0110111000	Lithuania	Pa	1001001111	Panama
lu	0110111010	Luxembourg	Pg	1001010110	Papua New Gui
mo	0110111110	Macau	Py	1001011000	Paraguay
mk	1100100111	Macedonia, Former Yu.	Pe	1001011100	Peru

Codificación de Dominios geográficos (continuación …….)

Dominio	Codificación	País	Dominio	Codificación	País
ph	1001100000	Philippines	th	1100000000	Thailand
pn	1001100100	Pitcairn Islands	tl	1001110010	Timor Leste
pl	1001101000	Poland	tg	1100000000	Togo
pt	1001101100	Portugal	tk	1100000100	Tokelau
pr	1001110110	Puerto Rico	to	1100001000	Tonga
					Trinidad and
qa	1001111010	Qatar	tt	1100001100	Toba.
re	1001111110	Réunion	tn	1100010100	Tunisia
ro	1010000010	Romania	tr	1100011000	Turkey
ru	1010000011	Russian Federation	tm	1100011011	Turkmenistan
rw	1010000110	Rwanda	tc	1100011100	Turks and Caic.
sh	1010001110	Saint Helena	tv	1100011110	Tuvalu
kn	1010010011	Saint Kitts and Nevis	ug	1100100000	Uganda
lc	1010010110	Saint Lucia	ua	1100100100	Ukraine
					United Arab
pm	1010011010	Saint Pierre and Miquel.	ae	1100010000	Emirat.
vc	1010011110	Saint Vincent and Gren.	gb	1100111010	United Kingdom
ws	1101110010	Samoa	us	1101001000	United Status
sm	1010100010	San Marino	um	1001000101	U.S. Minor Outl
st	1010100110	Sao Tome and Principe	uy	1101011010	Uruguay
sa	1010101010	Saudi Arabia	uz	1101011100	Uzbekistán
sn	1010101110	Senegal	vu	1000100100	Vanuatu
					Vatican City
cs	1101111011	Serbia and Montenegro	va	0101010000	State
sc	1010110010	Seychelles	ve	1101011110	Venezuela
sl	1010110110	Sierra Leone	vn	1011000000	Viet Nam
sg	1010111110	Singapore	vg	0001011100	Virgin Islands I.
sk	1010111111	Slovakia	vi	1101010010	Virgin Islands,
					Wallis and
si	1011000001	Slovenia	wf	1101101100	Futura
sb	0001011010	Solomon Islands	eh	1011011100	Western Sahara
so	1011000010	Somalia	ye	1101110111	Yemen
za	1011000110	South Africa	zm	1101111110	Zambia
gs	0011101111	South Georgia	zw	1011001100	Zimbabwe
es	1011010100	Spain			
lk	0010010000	Sri Lanka			
sd	1011100000	Sudan			
sr	1011100100	Suriname			
sj	1011101000	Svalbard and Jan May			
sz	1011101100	Swaziland			
se	1011110000	Sweden			
ch	1011110100	Switzerland			
sy	1011111000	Syrian Arab Republic			
tw	0010011110	Taiwan (Repu. of Ch.)			
tj	1011111010	Tajikistan			
Tz	1101000010	Tanzania, United Rep.			

Tabla # 5.12 Codificación del Remitente: Dominios Geográficos

TOTAL DE BITS UTILIZADOS **EN EL REMITENTE DEL MENSAJE**

[F2] = Caracteres del nombre de usuario + Número de subdominios + Dominio de más alto nivel

[F2] = 5 + 3 + 10 = **18 bits** del Remitente del Mensaje

[F2] = 18 bits

5.3.3 GENERACION DEL DESTINATARIO DEL MENSAJE

El formato que se genera para el envío del correo es el siguiente:

To: "'Danilo Pastor'" <danilopastor@andinanet.net>

Si es ***Destinatario*** **solamente es uno** entonces aplicamos las mismas reglas de codificación que las aplicadas en el ***Remitente*** y son:

- Número de caracteres del nombre de usuario
- Número de subdominios de la dirección de dominio
- Tipo de dominio de más alto nivel de la dirección de correo
- Y aumentamos 3 bits al final de los 18 bits

Si existen **varios destinatarios** se aplica la regla de codificación únicamente al primer destinatario, pero aumentamos al final 3 bits adicionales:

Codificación de Tipos de Destinatario

Cantidad de dígitos utilizados: **3**

Tipo de destinatario	Codificación
Uno solo / sin copia	111
Uno solo / con copia	110
Uno solo / con copia oculta	101
Varios / con copia	100
Varios / sin copia	011
Varios / con copia oculta	010
	001

Tabla # 5.13 Codificación del Destinatario: Tipo de Destinatario

TOTAL DE BITS UTILIZADOS **EN EL DESTINATARIO DEL MENSAJE**

[F3] = Caracteres del nombre de usuario + Número de subdominios + Dominio de más alto nivel + Tipo de Destinatario

[F3] = 5 + 3 + 10 + 3 = **21 bits** del Destinatario del Mensaje

[F3] = 21 bits

5.3.4 GENERACION DE LA PRIORIDAD DEL MENSAJE

El formato que se genera para la prioridad del mensaje de correo es el siguiente:

X-Priority: 3

La prioridad se define para dar la importancia de un mensaje de correo y existen solamente tres valores:

Codificación de Tipos de Prioridad

Cantidad de dígitos utilizados: **2**

Prioridad	Codificación
Alta	01
Normal	10
Baja	11

Tabla # 5.14 Codificación de la Prioridad del Mensaje

TOTAL DE BITS UTILIZADOS **EN LA PRIORIDAD DEL MENSAJE**

[F4] = Prioridad del mensaje = **2 bits** de la Prioridad del Mensaje

[F4] = 2 bits

5.3.5 GENERACION DE LOS DATOS ADJUNTOS

Los datos adjuntos conocidos como *attachment* son una de las características más utilizadas en el envió de mensajes de correo electrónico y solamente verificaremos si existen o no archivos adjuntos en el mensaje:

Codificación de Datos Adjuntos

Cantidad de dígitos utilizados: **2**

Datos Adjuntos	Codificación
No	01
Un solo	10
Mas de uno	11

Tabla # 5.15 Codificación de los Datos Adjuntos del Mensaje

TOTAL DE BITS UTILIZADOS **EN LOS DATOS ADJUTNOS DEL MENSAJE**

[F5] = Codificación de Datos adjuntos = **2 bits** de los Datos adjutnos

[F5] = 2 bits

5.3.6 GENERACION LA CANTIDAD DE CARACTERES DEL ASUNTO

El formato que se genera para el envío del correo es el siguiente:

Subject: Re: Multiproyecto de Accion Global

Cantidad Caracteres producidos por el campo Asunto

Codificamos de acuerdo a la cantidad de caracteres que tenga el nombre de usuario

Codificación

Número de Caracteres	Codificación
01	00000001
02	00000010
03	00000011
04	00000100
05	00000101
06	00000110
07	00000111
08	00001000
09	00001001
10	00001010
.	.
.	.
255	11111111

Tabla # 5.16 Codificación de la cantidad de caracteres del campo Asunto

Cantidad de dígitos utilizados: **8**

TOTAL DE BITS UTILIZADOS **EN LA CANTIDAD DE CARACTERES DEL ASUNTO**

[F6] = Cantidad de caracteres que contenga el campo Asunto = **8 bits**

[F6] = 8 bits

5.3.7 CANTIDAD DE BITS PARA COMPLETAR LA CLAVE

Repetimos los 28 primeros bits producidos en la generación de la fecha y hora del mensaje

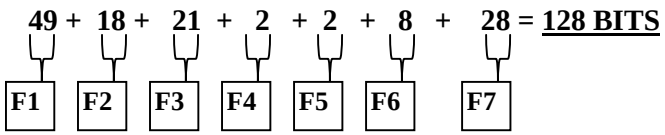
Cantidad de dígitos utilizados: **28**

TOTAL DE BITS UTILIZADOS **PARA COMPLETAR LA CLAVE**

[F7] = Cantidad de bits para completar la clave = **28 bits**

[F7] = 28 bits

TOTAL GENERAL PARA LA GENERACION DE LA CLAVE DE 128 BITS:



En donde F? está detallado a continuación:

- Fecha de envío del mensaje ---------- F1
- Remitente ---------- F2
- Destinatario (uno o múltiples, con copia) ---------- F3
- Prioridad ---------- F4
- Datos adjuntos ---------- F5
- Cantidad de caracteres en el asunto (Subject) ------ F6
- Cantidad de bits para completar la clave ---------- F7

5.4 ENCUBRIMIENTO DE LA CLAVE

Para evitar que la clave sea aún difícil de obtener se aplica los conceptos de confusión y difusión, haciendo uso de las siguientes operaciones elementales:

- Permutación
- XOR.

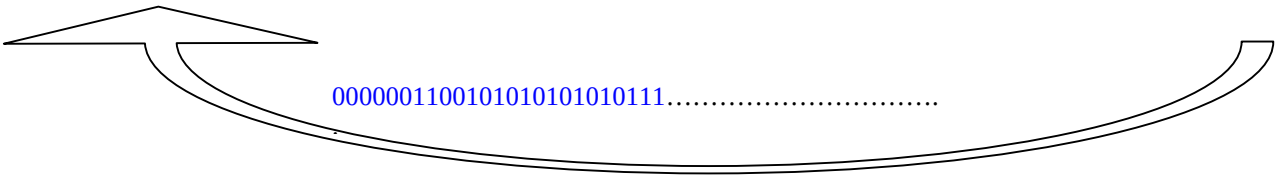
El procedimiento es sencillo y simplemente se realiza una permutación (rotación) a la clave generada de 25 bits a la derecha para posteriormente realizar la operación XOR con la clave original generada.

Permutación

10010001101000110100100000011111……000111010101010101001100000 0

Clave Generada de 128 bits

Permutamos (rotamos) 25 bits a la derecha



El resultado quedaría así:

11101010101010100110000001001000110100011010010000000111111……1100000

Clave Permutada de 128 bits

XOR

Aplicamos la función lógica XOR de acuerdo a la tabla de equivalencias siguiente:

ENTRADAS		SALIDA
A	**B**	**XOR**
0	0	0
1	0	1
0	1	1
1	1	0

Tabla # 5.17 Tabla de equivalencias de la Operación lógica XOR

Entonces realizamos la operación XOR entre *La Clave Generada* y *La Clave Permutada*

100100011010001101001000000011111……000111010101010101001100000**0**

xor

111010101010101001100000**0**10010001101000110100100000011111……1100000

01111011000010010010100001000111101……..1001110110101……0100000

Clave Resultante de 128 bits

Con esta clave se procede a la encriptación del Mensaje de correo utilizando el algoritmo IDEA.

5.5 ENCRIPTACION UTILIZANDO EL ALGORITMO IDEA

El algoritmo IDEA (International Data Encryption Algorithm). Tomando en cuenta que para muchos constituye el mejor y más seguro algoritmo simétrico disponible en la actualidad. Trabaja con bloques de 64 bits de longitud y emplea una clave de 128 bits. Se usa el mismo algoritmo tanto para cifrar como para descifrar.

IDEA es un algoritmo bastante seguro, y hasta ahora se ha mostrado resistente a multitud de ataques, entre ellos el criptoanálisis diferencial.

No presenta claves débiles, y su longitud de clave hace imposible en la práctica un ataque por la fuerza bruta.

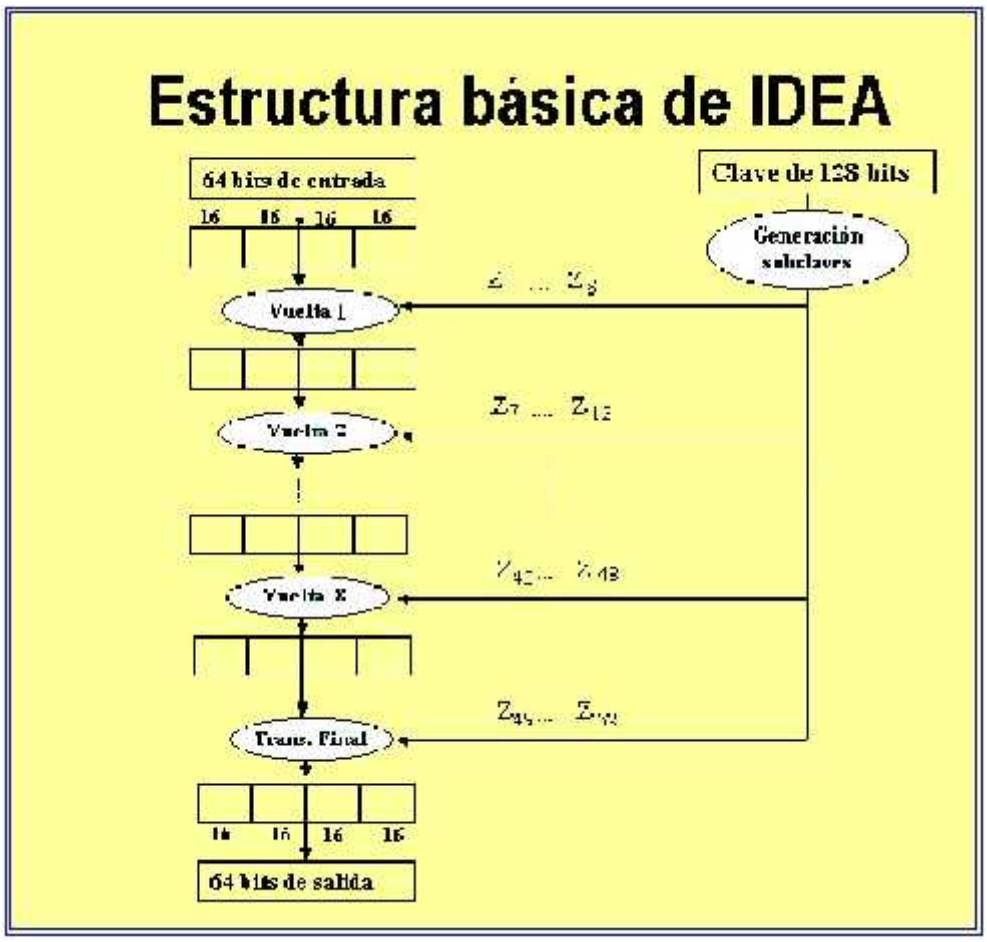


Figura # 5.3 Gráfico de la Estructura Básica del Algoritmo IDEA

Como ocurre con todos los algoritmos simétricos de cifrado por bloques, IDEA se basa en los conceptos de confusión y difusión, haciendo uso de las siguientes operaciones elementales (todas ellas fáciles de implementar):

- XOR.
- Suma módulo 2^{16}.
- Producto módulo $2^{16} + 1$.

El algoritmo IDEA consta de ocho rondas. Dividiremos el bloque X a codificar, de 64 bits, en cuatro partes X_1, X_2, X_3 y X_4 de 16 bits. Para la interpretación entera de dichos registros se empleará el criterio *big endian*, lo cual significa que el primer *byte* es el más significativo. Denominaremos Z_i a cada una de las 52 subclaves de 16 bits que vamos a necesitar. Las operaciones que llevaremos a cabo en cada ronda son las siguientes:

1. Multiplicar X_1 por Z_1.
2. Sumar X_2 con Z_2.
3. Sumar X_3 con Z_3.
4. Multiplicar X_4 por Z_4.
5. Hacer un XOR entre los resultados del paso 1 y el paso 3.
6. Hacer un XOR entre los resultados del paso 2 y el paso 4.
7. Multiplicar el resultado del paso 5 por Z_5.
8. Sumar los resultados de los pasos 6 y 7.
9. Multiplicar el resultado del paso 8 por Z_6.
10. Sumar los resultados de los pasos 7 y 9.
11. Hacer un XOR entre los resultados de los pasos 1 y 9.
12. Hacer un XOR entre los resultados de los pasos 3 y 9.
13. Hacer un XOR entre los resultados de los pasos 2 y 10.
14. Hacer un XOR entre los resultados de los pasos 4 y 10.

La salida de cada iteración serán los cuatro sub-bloques obtenidos en los pasos 11, 12, 13 y 14, que serán la entrada del siguiente ciclo, en el que emplearemos las siguientes seis subclaves, hasta un total de 48. Al final de todo intercambiaremos los dos bloques centrales (en realidad con eso *deshacemos* el intercambio que llevamos a cabo en los pasos 12 y 13).

Después de la octava iteración, se realiza la siguiente transformación:

1. Multiplicar X_1 por Z_{49}.
2. Sumar X_2 con Z_{50}.
3. Sumar X_3 con Z_{51}.
4. Multiplicar X_4 por Z_{52}.

Las primeras ocho subclaves se calculan dividiendo la clave de entrada en bloques de 16 bits. Las siguientes ocho se calculan rotando la clave de entrada 25 bits a la izquierda y volviendo a dividirla, y así sucesivamente.

Las subclaves necesarias para descifrar se obtienen cambiando de orden las Zi y calculando sus inversas para la suma o la multiplicación, según la tabla # 5.18. Puesto que $2^{16} + 1$ es un número primo, nunca podremos obtener cero como producto de dos números, por lo que no necesitamos representar dicho valor. Cuando estemos calculando productos, utilizaremos el cero para expresar el número 2^{16} —un uno seguido de 16 ceros—. Esta representación es coherente puesto que los registros que se emplean internamente en el algoritmo poseen únicamente 16 bits.

Ronda	**Subclaves de cifrado**						**Suclaves de Decifrado**					
1	Z_1	Z_2	Z_3	Z_4	Z_5	Z_6	Z_{49}^{-1}	$-Z_{50}$	$-Z_{51}$	Z_{52}^{-1}	Z_{47}	Z_{48}
2	Z_7	Z_8	Z_9	Z_{10}	Z_{11}	Z_{12}	Z_{43}^{-1}	$-Z_{45}$	$-Z_{44}$	Z_{46}^{-1}	Z_{41}	Z_{42}
3	Z_{13}	Z_{14}	Z_{15}	Z_{16}	Z_{17}	Z_{18}	Z_{37}^{-1}	$-Z_{39}$	$-Z_{38}$	Z_{40}^{-1}	Z_{35}	Z_{36}
4	Z_{19}	Z_{20}	Z_{21}	Z_{22}	Z_{23}	Z_{24}	Z_{31}^{-1}	$-Z_{33}$	$-Z_{32}$	Z_{34}^{-1}	Z_{29}	Z_{30}
5	Z_{25}	Z_{26}	Z_{27}	Z_{28}	Z_{29}	Z_{30}	Z_{25}^{-1}	$-Z_{27}$	$-Z_{26}$	Z_{28}^{-1}	Z_{23}	Z_{24}
6	Z_{31}	Z_{32}	Z_{33}	Z_{34}	Z_{35}	Z_{36}	Z_{19}^{-1}	$-Z_{21}$	$-Z_{20}$	Z_{22}^{-1}	Z_{17}	Z_{18}
7	Z_{37}	Z_{38}	Z_{39}	Z_{40}	Z_{41}	Z_{42}	Z_{13}^{-1}	$-Z_{15}$	$-Z_{14}$	Z_{16}^{-1}	Z_{11}	Z_{12}
8	Z_{43}	Z_{44}	Z_{45}	Z_{46}	Z_{47}	Z_{48}	Z_7^{-1}	$-Z_9$	$-Z_8$	Z_{10}^{-1}	Z_5	Z_6
Final	Z_{49}	Z_{50}	Z_{51}	Z_{52}			Z_1^{-1}	$-Z_2$	$-Z_3$	Z_4^{-1}		

Tabla # 5.18 Subclaves empleadas en el Algoritmo IDEA

CAPITULO VI

DESARROLLO DE UN PROTOTIPO CLIENTE DE CORREO ELECTRONICO

6.1 ANALISIS Y DISEÑO ORIENTADO A OBJETOS

Una de las tareas más difíciles que se encuentra el desarrollador durante el avance de un sistema, es la abstracción del mundo real de lo que en contexto se desea construir, y que aquello se identifique en un alto porcentaje con los requerimientos de los clientes, de esta manera se creará un sistema que ayude a simplificar los problemas y las necesidades del usuario final.

De lo anteriormente expresado la parte más compleja es representar ese mundo real a través de un lenguaje entendible tanto para el desarrollador como para el usuario.

Desde hace mucho tiempo atrás, se ha venido acarreando este problema de no contar con un lenguaje universal, en que su representación sea comprendida y entendida por la gran mayoría de desarrolladores y además se adapte a las exigencias actuales. Por esta y otras muchas razones se

creó el lenguaje UML como un conjunto de diagramas para representar las necesidades de los usuarios. Por ende para el desarrollo del Sistema Cliente de Correo se utilizará dicho lenguaje tanto en la fase de análisis como en la fase de diseño.

Tomando en cuenta que uno de los pilares fundamentales en cualquier sistema de calidad es sin duda el análisis previo al diseño, es considerado como una fase indispensable que sirve para modelar a través de un lenguaje técnico los requerimientos de los usuarios, de esta manera el desarrollador no cometerá el error de construir una solución elegante para un problema equivocado.

Para contrarrestar el error anteriormente mencionado hay que partir de una concepción claramente establecida, la cual da a entender que no se puede construir software hasta que no se tiene un conocimiento razonable del sistema. Por lo que es conveniente partir de un modelo evolutivo en que, en las distintas fases se pueda ir refinando el sistema mediante el desarrollo de varias versiones.

Sin embargo cabe recalcar que todas las fases de la ingeniería como el análisis y el diseño están inmersas dentro de un modelo de desarrollo de software, de lo que se ha considerado conveniente escoger el **Modelo de Prototipos** para el desarrollo de este sistema, el cual consiste en varias versiones mejoradas del mismo.

Aunque el desarrollo del sistema ha sido realizado por una sola persona, se puede contemplar que algunas tareas han sido realizadas paralelamente a otras complementándose así en las distintas fases de la ingeniería del software.

En conclusión, el objetivo de esta fase es tener una mejor comprensión de los requerimientos a diseñar, los mismos que luego de ser refinados serán plasmados en la aplicación final.

6.2 ANALISIS DE REQUERIMIENTOS DEL CLIENTE DE CORREO

En términos generales, el Sistema deberá proporcionar soporte a las siguientes tareas de gestión de Correo Electrónico:

- Gestión de cuentas de correo electrónico
- Gestión de creación de mensajes de correo electrónico
- Gestión de lectura de mensajes de correo electrónico
- Gestión de envío y recepción de correo electrónico
- Gestión de encriptación de correo electrónico

Se presentan los requisitos funcionales que deberán ser satisfechos por el sistema. Todos los requisitos aquí expuestos son ESENCIALES, es decir, no sería aceptable un sistema que no satisfaga alguno de los requisitos aquí presentados. Estos requisitos se han especificado teniendo en cuenta, entre otros, el criterio de "testabilidad": dado un requisito, debería ser fácilmente demostrable si es satisfecho o no por el sistema.

6.2.1 REQUISITOS FUNCIONALES

GESTIÓN DE CUENTAS DE CORREO ELECTRONICO

Req(01) Cada vez que se desee enviar o recibir un e-mail se necesita primeramente configurar una cuenta de correo para poder conectarse al servidor de Correo. Se deberá permitir la posibilidad de configurar algunas cuentas de correo y seleccionar cual es la cuenta por defecto a utilizar. Además se deberá permitir eliminar una cuenta ya existente. También se tendrá la posiblidad de cambiar la configuración de la cuentas ya creadas.

Req(02) La configuración de una cuenta de correo deberá permitir recopilar características de como la información del usuario, nombre de la cuenta, servidor de correo entrante y saliente, nombre del usuario y su password, y además los puertos utilizados por los servicios de correo y su tiempo máximo de espera.

GESTIÓN DE CREACION DE MENSAJES DE CORREO ELECTRONICO

Req(03) El Sistema permitirá crear mensajes nuevos mediante una interfaz que se pueda especificar el destinatario, las copias a los usuarios que se desee enviar, el asunto (título) del mensaje, y el contenido del mensaje propiamente dicho.

Req(04) El Sistema permitirá además configurar ciertas propiedades adicionales en la creación de mensajes, como añadir archivos, escoger un nivel de prioridad, escoger el tipo de contenido del adjunto, etc.

Req(05) Cuando esté debidamente redactado un mensaje se deberá dar la posibilidad de enviarlo inmediatamente al Servidor de correo saliente para que éste a su vez, se encargue de entregarlo a su destino.

GESTIÓN DE LECTURA DE MENSAJES DE CORREO ELECTRONICO

Req(06) El Usuario podrá apreciar mediante algún tipo de listado los encabezados de los mensajes que tiene en su Servidor de correo entrante para poder seleccionar el mensaje que desea examinar.

Req(07) Cuando el usuario seleccione un mensaje de correo, se le deberá dar la posibilidad de visualizar todo el contenido del mensaje, incluyendo sus características adicionales como la descarga de archivos adjuntos, si existe de archivos adjuntos.

Req(08) Se debe dar la posibilidad al usuario que pueda responder o reenviar el mensaje que está visualizando.

GESTIÓN DE ENVIO Y RECEPCION DE MENSAJES DE CORREO ELECTRONICO

Req(09) El usuario debe tener la posibilidad de interactuar para poder enviar y visualizar los mensajes de correo hacia y desde el Servidor de correo Electrónico respectivamente.

Req(10) El usuario debe tener la posibilidad de eliminar un mensaje del servidor de correo, imprimirlo, etc.

GESTIÓN DE ENCRIPTACION DE CORREO ELECTRONICO

Req(11) Debe existir la posibilidad de enviar y recibir mensajes encriptados, por defecto, pasando por desapercibido para el usuario.

Req(12) Debe transmitirse los mensajes de correo por los diferentes Servidores de Correo ya encriptados y sujetándose a los estándares de correo respectivos.

Req(13) No debe haber la posibilidad de que los mensajes enviados puedan abrirse desde cualquier otro Cliente de Correo, solo se puede abrir desde la Propuesta de Correo.

6.2.2 REQUISITOS TECNOLOGICOS

El Cliente de Correo se ejecutará sobre un PC con una configuración mínima de:

- Procesador: Pentium 200 Mhz.
- Memoria: 64 Mb
- Espacio libre en disco: 10 Mb.
- Tarjeta Ethernet o Módem o Tarjeta RDSI

El sistema operativo sobre el que se debe ejecutar la aplicación es Windows9X, Windows 2000, Windows XP.

La aplicación debe ser independiente del Servidor de Correo que se utilice, aunque sí es requisito que soporte los estándares de correo como son SMTP, y POP3.

6.3 DEFINICION DE LOS CASOS DE USO

Los casos de uso nos ayudan en forma general a describir un escenario de software que va a ser usado en una determinada situación, convirtiéndose en una técnica excelente para la comprensión de los requerimientos, es decir, narraciones de los procesos del dominio. Los casos de uso son descripciones o casos de utilización de un sistema; no son exactamente los requerimientos ni las especificaciones funcionales, sino que ejemplifica e incluyen tácitamente los requerimientos en las descripciones.

Para el Sistema Cliente de Correo ha sido conveniente describir todo el proceso generalizado en un caso de uso de alto nivel esencial, y a partir de este definir los demás casos de uso en formato expandido que son necesarios para el óptimo desarrollo del sistema.

6.3.1 CASO DE USO DE ALTO NIVEL ESENCIAL

NOMBRE: Proceso de envío de mensajes de correo electrónico.

ACTORES: Usuario emisor, Usuario receptor.

TIPO: Primario.

DESCRIPCIÓN:

El usuario emisor es quién inicia la iteración cuando elige enviar un nuevo e-mail mediante el sistema Cliente de correo, pero antes debe iniciar su cuenta de correo, si ya se encuentra en su cuenta activa deberá escribir el o los destinatarios de ese e-mail, el asunto al que se refiere el mensaje de correo, el cuerpo mismo del mensaje, luego el usuario emisor puede escoger las siguientes opciones como adjuntar un archivo existente, escoger la prioridad, definir si el mensaje será enviado con encriptación o sin encriptación y finalmente el usuario emisor elige enviar el

mensaje. Internamente el sistema se encarga de encriptar el mensaje (si esa opción ha sido escogida) usando el algoritmo simétrico (IDEA) para obtener un mensaje cifrado. Mediante el agente de transferencia de correo (MTA) el usuario receptor recibe el mensaje, pero antes el usuario receptor deberá iniciar su cuenta de correo en el sistema Cliente de correo, caso contrario si el mensaje ha sido encriptado ninguna otra aplicación podrá mostrar el contenido de dicho mensaje. Internamente el sistema Cliente de correo se encarga de desencriptar el mensaje cifrado recibido mediante el algoritmo simétrico (IDEA) y mostrar al usuario receptor el mensaje original. Tanto el usuario emisor como el usuario receptor pueden responder o reenviar un mensaje cualquiera, teniendo en cuenta que el proceso es similar al anteriormente descrito salvo que en el proceso de responder el sistema pone por defecto la cuenta correspondiente del mensaje que se va a responder, y en caso de reenviar el usuario puede escribir a quien o quienes desea reenviar el mensaje.

6.3.2 DIAGRAMA DE CASOS DE USO

A continuación se presentan todos los casos de uso más representativos del sistema Cliente de correo con la representación gráfica de cada uno, tomando en cuenta que este tipo de diagramas nos permite identificar gráficamente la interacción entre los Actores(Usuarios) y el sistema (Cliente de Correo), donde representan en forma general o específica la funcionalidad del sistema propuesto.

NOMBRE:	Crear o agregar nueva cuenta
CÓDIGO:	CU_01
ACTORES:	Usuario
TIPO:	Primario, Esencial
VISIÓN GENERAL:	Crear o agregar una nueva cuenta de correo electrónico.

REFERENCIAS:	Ninguna
CURSO TÍPICO DE EVENTOS:	
ACTORES	**SISTEMA**
1. El usuario solicita agregar una nueva cuenta.	2. Presenta un cuadro de propiedades de cuenta (General, Servidores, Opciones avanzadas) y por defecto la ficha General.
3. El usuario llena ficha General con los datos correspondientes a nombre de la cuenta e información de usuario (Nombre, Organización, Dirección de correo electrónico, Dirección de respuesta), luego el usuario escoge la ficha Servidores.	4. Presenta la ficha Servidores.
5. El usuario llena ficha Servidores con los datos correspondientes a Correo entrante, Correo saliente, Nombre de la cuenta y Contraseña, consecuentemente el usuario escoge la ficha Opciones avanzadas.	6. Presenta la ficha Opciones avanzadas.
7. El usuario puede modificar en la ficha Opciones avanzadas los parámetros de Correo saliente, Correo entrante, e inclusive establecer el Tiempo de espera. Finalmente el usuario solicita guardar la cuenta.	8. Se almacenan los datos de la cuenta, se crea la misma y se agrega a un listado donde se encuentran todas las cuentas creadas.

Tabla # 6.1 Descripción del Caso de Uso – Crear o agregar nueva cuenta

Diagrama de CU_01:

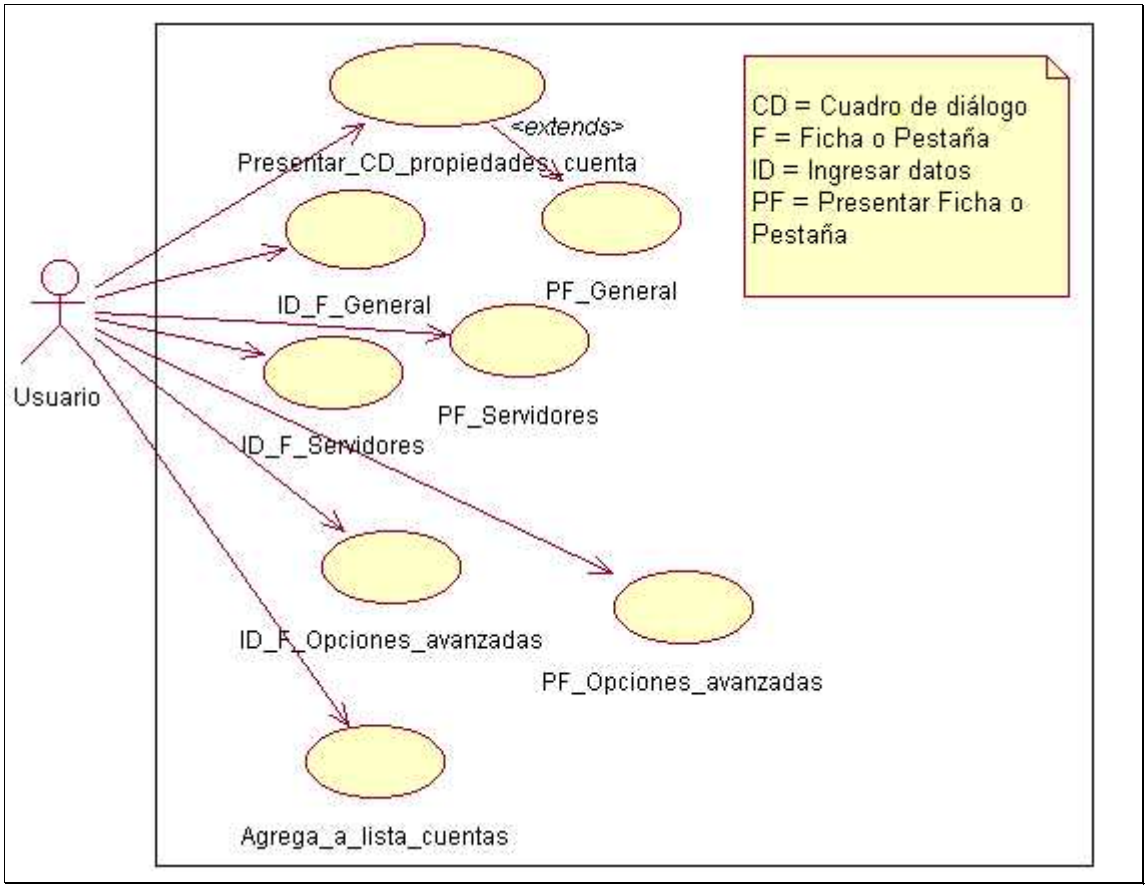


Figura # 6.1 Casos de Uso CU_01: Crear o agregar una nueva cuenta.

NOMBRE:	Operaciones con cuentas
CÓDIGO:	CU_02
ACTORES:	Usuario
TIPO:	Primario, Esencial
VISIÓN GENERAL:	De una lista de cuentas creadas permitir al usuario agregar, quitar establecer como predeterminada una cuenta o cambiar las propiedades de una cuenta en particular.
REFERENCIAS:	CU_01

CURSO TÍPICO DE EVENTOS:

ACTORES	**SISTEMA**
1. El usuario solicita mostrar todas las cuentas existentes.	2. Muestra todas las cuentas existentes con su respectivo tipo (predeterminada o no) y conexión. Además presenta las opciones de operación con cuentas (Agregar, Quitar, Predeterminada, Propiedades).
3. El usuario escoge la opción Agregar.	4. Presenta un cuadro de propiedades descrito en el caso de uso de código CU_01.
5. Terminada la operación anterior el	6. Elimina la cuenta seleccionada.

usuario solicita quitar una cuenta en particular seleccionándola de la lista y escogiendo la opción Quitar.	
	8. Realiza operaciones internas y establece la cuenta seleccionada como predeterminada.
7. El usuario desea establecer como predeterminada una cuenta, la selecciona de la lista y escoge la opción Predeterminada.	
9. El usuario solicita mostrar las propiedades de una cuenta en particular escogiendo la opción Propiedades.	10. Muestra las propiedades de la cuenta seleccionada.
11. El usuario solicita cambiar los datos de la cuenta, para lo que ingresa nuevos datos o modifica los existentes.	12. Almacena los cambios realizados si los hay.

Tabla # 6.2 Descripción del Caso de Uso – Operaciones con cuentas

Diagrama de CU_02:

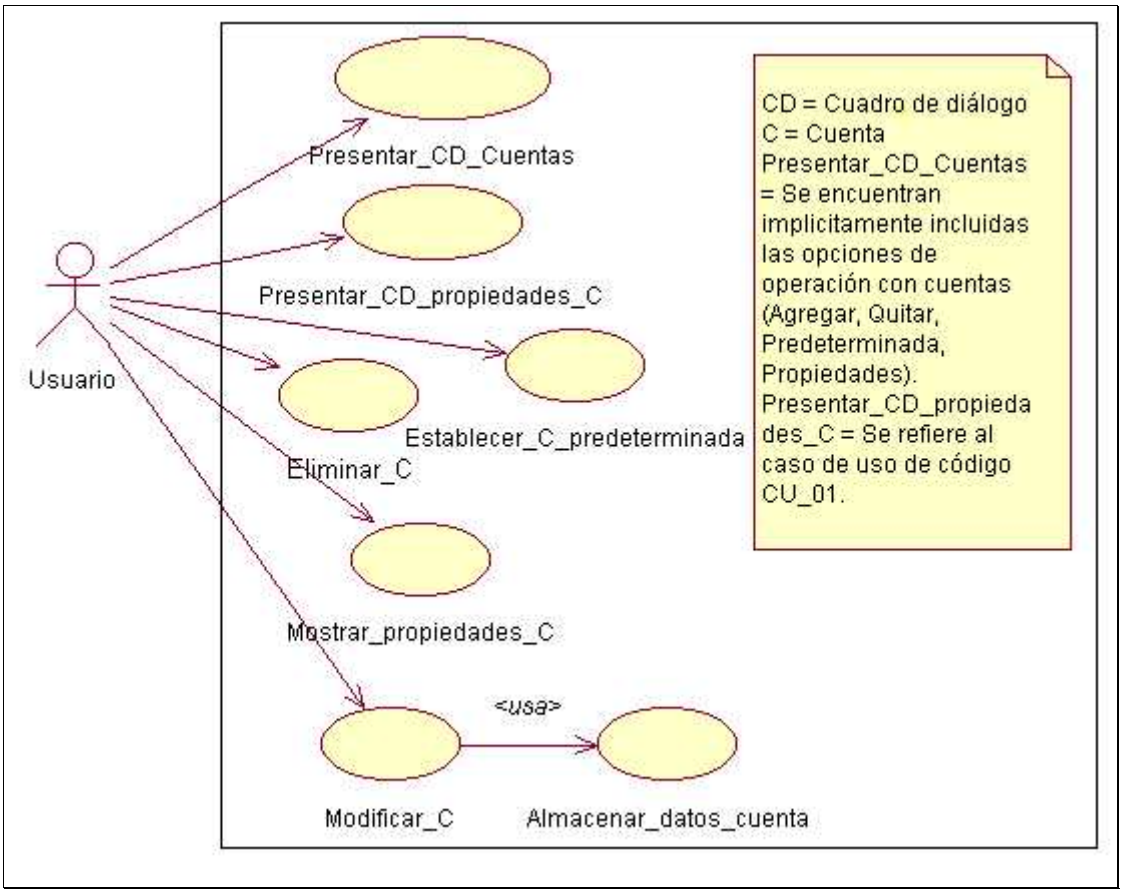


Figura # 6.2 Casos de Uso CU_02: Operaciones con cuentas.

NOMBRE:	Enviar nuevo e-mail

CÓDIGO:	CU_03
ACTORES:	Usuario
TIPO:	Primario, Esencial
VISIÓN GENERAL:	El usuario crea un nuevo e-mail, para luego enviarlo a un destinatario en particular.
REFERENCIAS:	CU_04

CURSO TÍPICO DE EVENTOS:

ACTORES	**SISTEMA**
1. El usuario solicita crear un nuevo mensaje de correo electrónico escogiendo la opción Nuevo.	2. Presenta un cuadro de diálogo de Enviar e-mail con todas las opciones (Adjuntar un archivo existente, imprimir, escoger la prioridad, encriptar o no el mensaje y enviar) necesarias para dicha operación y datos que tiene que llenar el usuario.
3. El usuario llena los datos necesarios como el destinatario o los campos CC o Bcc, el asunto, y el cuerpo mismo del mensaje a enviar. Además el usuario escoge las opciones de prioridad y encriptación. Si el usuario desea enviar el e-mail ya puede hacerlo escogiendo la opción enviar, pero si el usuario desea adjuntar un archivo escoge la opción Adjuntar.	4. Presenta un cuadro de diálogo Abrir donde puede el usuario puede escoger el archivo deseado.
5. El usuario selecciona el archivo a adjuntar.	6. Adjunta el archivo al e-mail.
7. Si el usuario desea adjuntar otro archivo repite el proceso anteriormente explicado. Luego el usuario solicita imprimir el mensaje.	8. Presenta opciones de impresora y luego imprime el mensaje. Proceso descrito en el caso de uso de código CU_04
9. Finalmente el usuario escoge la opción de Enviar el e-mail.	10. Realiza las operaciones, validaciones y verificaciones necesarias. Si: se encuentra todo correcto el mensaje es enviado a su o sus destinatarios. No: se encuentra todo correcto se presenta un mensaje de error, enunciando la causa del error.

Tabla # 6.3 Descripción del Caso de Uso – Enviar nuevo mail

Diagrama de CU_03:

.

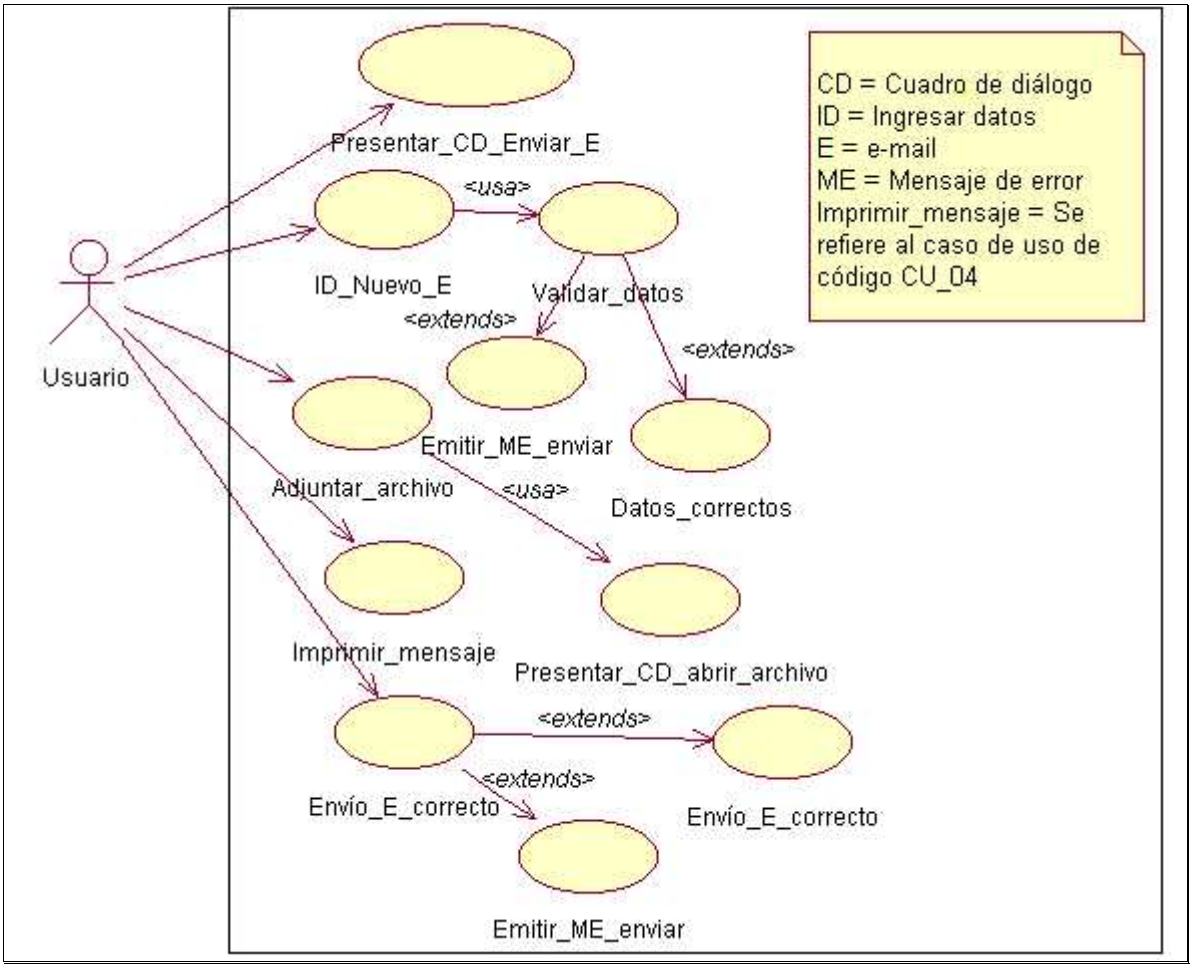


Figura # 6.3 Casos de Uso CU_03: Enviar un nuevo e-mail

NOMBRE:	Imprimir e-mail
CÓDIGO:	CU_04
ACTORES:	Usuario
TIPO:	Secundario
VISIÓN GENERAL:	Imprimir mediante el sistema, un e-mail cualquiera de las carpetas locales.
REFERENCIAS:	

CURSO TÍPICO DE EVENTOS:

ACTORES	**SISTEMA**
1. El usuario solicita imprimir un e-mail seleccionado en particular.	2. Presenta un cuadro de diálogo para establecer las propiedades de la impresora.
3. Acepta o modifica las propiedades de la impresora y elige imprimir.	4. Imprime el documento correspondiente.
5. Recibe la información impresa.	

Tabla # 6.4 Descripción del Caso de Uso – Imprimir e-mail

Diagrama de CU_04:

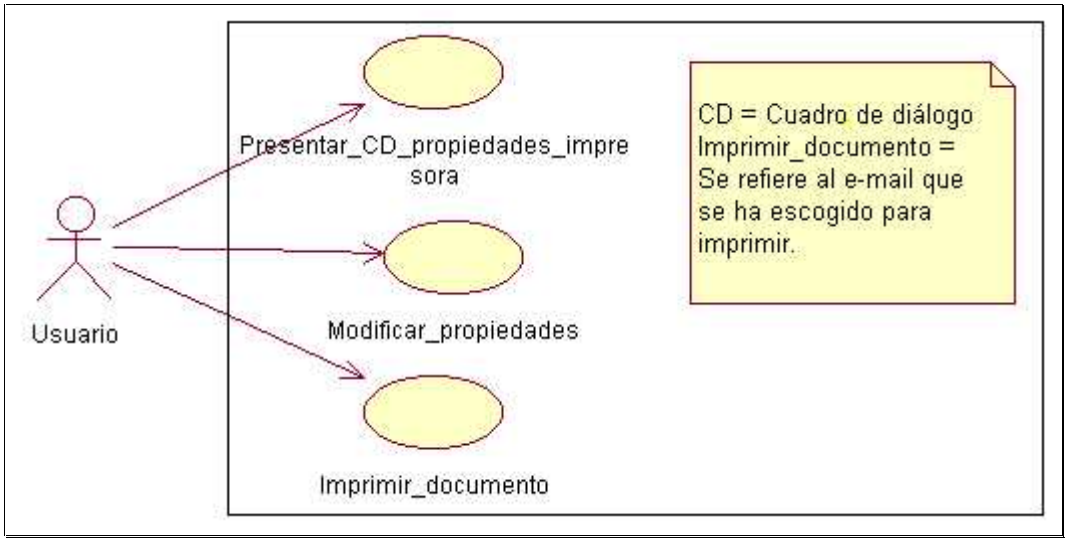


Figura # 6.4 Casos de Uso CU_04: Imprimir un e-mail

NOMBRE:	Eliminar e-mail
CÓDIGO:	CU_05
ACTORES:	Usuario
TIPO:	Secundario
VISIÓN GENERAL:	Elimina mediante el sistema, un e-mail cualquiera de las carpetas locales.
REFERENCIAS:	
CURSO TÍPICO DE EVENTOS:	
ACTORES	**SISTEMA**
1. El usuario solicita eliminar un e-mail seleccionado en particular. 3. El usuario sigue con otras actividades en el sistema.	2. Elimina el e-mail seleccionado y se registra en elementos eliminados de carpetas locales.

Tabla # 6.5 Descripción del Caso de Uso – Eliminar e-mail

Diagrama de CU_05:

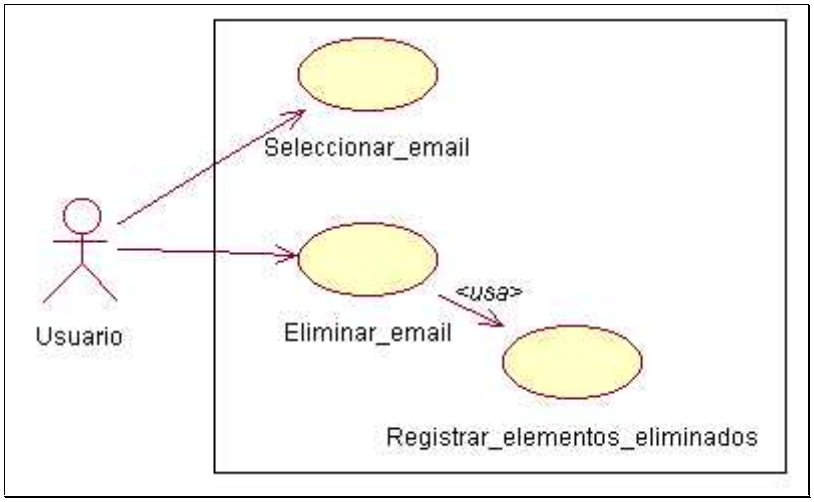


Figura # 6.5 Casos de Uso CU_05: Eliminar un e-mail

NOMBRE:	Mostrar e-mail
CÓDIGO:	CU_07
ACTORES:	Usuario
TIPO:	Primario
VISIÓN GENERAL:	Permite mostrar la información que contiene un e-mail independientemente de donde se ubique (Bandeja de entrada, Bandeja de salida, Elementos enviados, Elementos eliminados, Borrador).
REFERENCIAS:	

CURSO TÍPICO DE EVENTOS:

ACTORES	**SISTEMA**
1. El usuario solicita ver la información de un e-mail en particular. 3. El usuario visualiza la información y puede imprimir, contestar o reenviar el e-mail en cuestión.	2. Muestra la información del e-mail seleccionado

Tabla # 6.6 Descripción del Caso de Uso – Mostrar e-mail

Diagrama de CU_07:

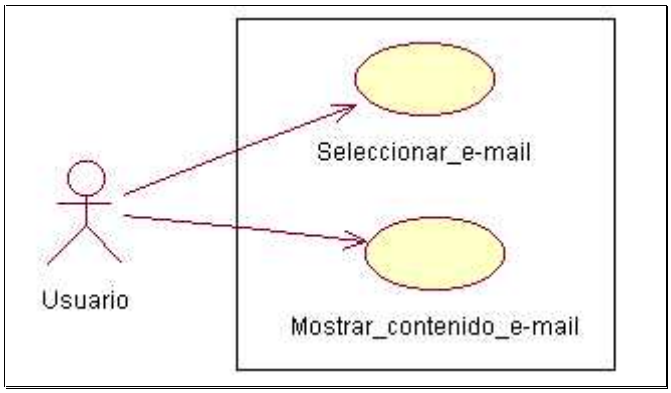


Figura # 6.7 Casos de Uso CU_07: Mostrar un e-mail

NOMBRE:	Enviar y recibir e-mail
CÓDIGO:	CU_08

ACTORES:	Usuario
TIPO:	Primario, Esencial
VISIÓN GENERAL:	Similar a una actualización general de toda la información de las carpetas locales.
REFERENCIAS:	

CURSO TÍPICO DE EVENTOS:

ACTORES	**SISTEMA**
1. El usuario elige la opción enviar y recibir. 3. El usuario revisa la nueva información.	2. Realiza la conexión con el servidor durante un corto tiempo, se termina la conexión y presenta nuevos e-mail si los hay.

Tabla # 6.7 Descripción del Caso de Uso – Enviar y recibir e-mail

Diagrama de CU_08:

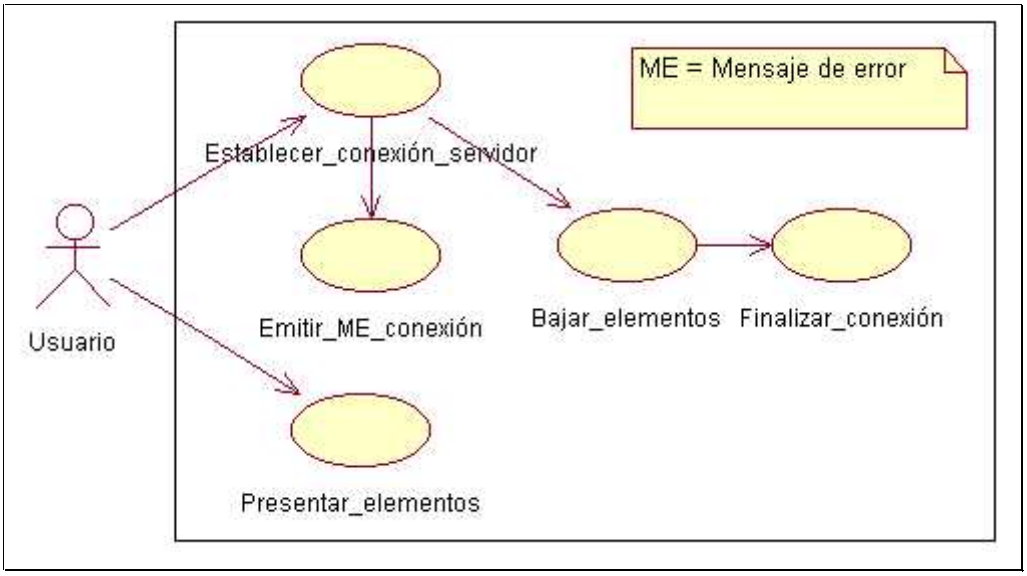


Figura # 6.8 Casos de Uso CU_08: Enviar y recibir un e-mail

NOMBRE:	Manejo de errores
CÓDIGO:	CU_10
ACTORES:	Usuario
TIPO:	Primario
VISIÓN GENERAL:	Se encarga de validar y verificar antes de cada operación para indicar si existen errores en el proceso mediante mensajes de error. El manejo de errores no solo se refiere a errores de sintaxis como no escribir correctamente el nombre del destinatario, sino que además también está encargado de los errores de conexión.
REFERENCIAS:	

CURSO TÍPICO DE EVENTOS:

ACTORES	SISTEMA
1. El usuario en una operación dentro del sistema ingresa datos luego solicita seguir con dicha operación.	2. Valida y verifica los datos según la operación que el usuario desea realizar. Si: todo esta correcto se continúa con la ejecución de la operación. No: están correctos los datos se emite un mensaje de error indicando el error que se ha cometido.
3. El usuario se encuentra realizando operaciones que tienen que ver con la conexión con el servidor y solicita seguir con dicha operación.	4. Verifica la conexión con el servidor y muchos aspectos que pueden afectar a la misma. Si: la conexión ha sido satisfactoria se sigue con la operación. No: ha sido posible la conexión con el servidor por varios factores se emite un mensaje de error indicando el posible error.

Tabla # 6.8 Descripción del Caso de Uso – Manejo de errores

Diagrama de CU_10:

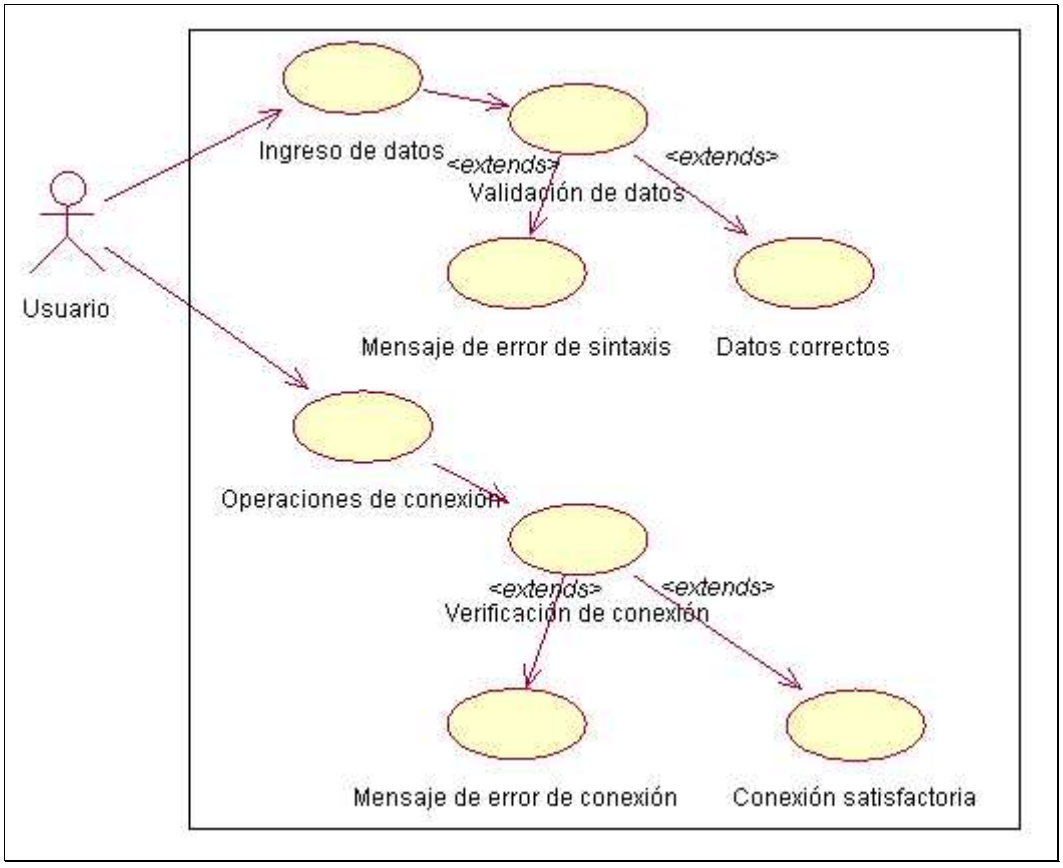


Figura # 6.10 Casos de Uso CU_10: Manejo de errores

6.4 DIAGRAMA DE ITERACION

6.4.1 DIAGRAMA DE SECUENCIA

Permiten representar desde otro punto de vista la secuencia de forma ordenada de cómo el usuario interactúa directamente con el sistema Cliente de Correo.

Cada diagrama de secuencia está asociado con un respectivo caso de uso, de lo que se trata de representar los servicios que ofrece el sistema propuesto.

Diagrama de Secuencia 02:

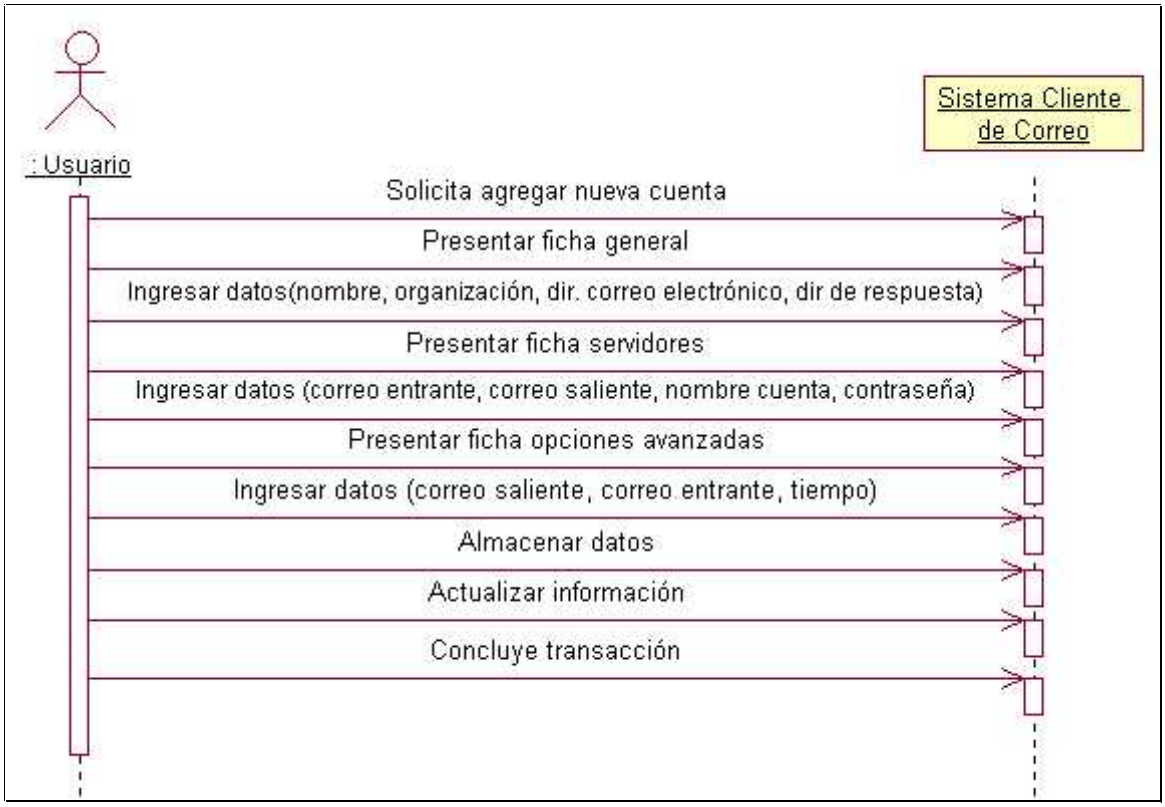


Figura # 6.11 Diagrama de Secuencia 02 (Caso de Uso CU_02)

Diagrama de Secuencia 03:

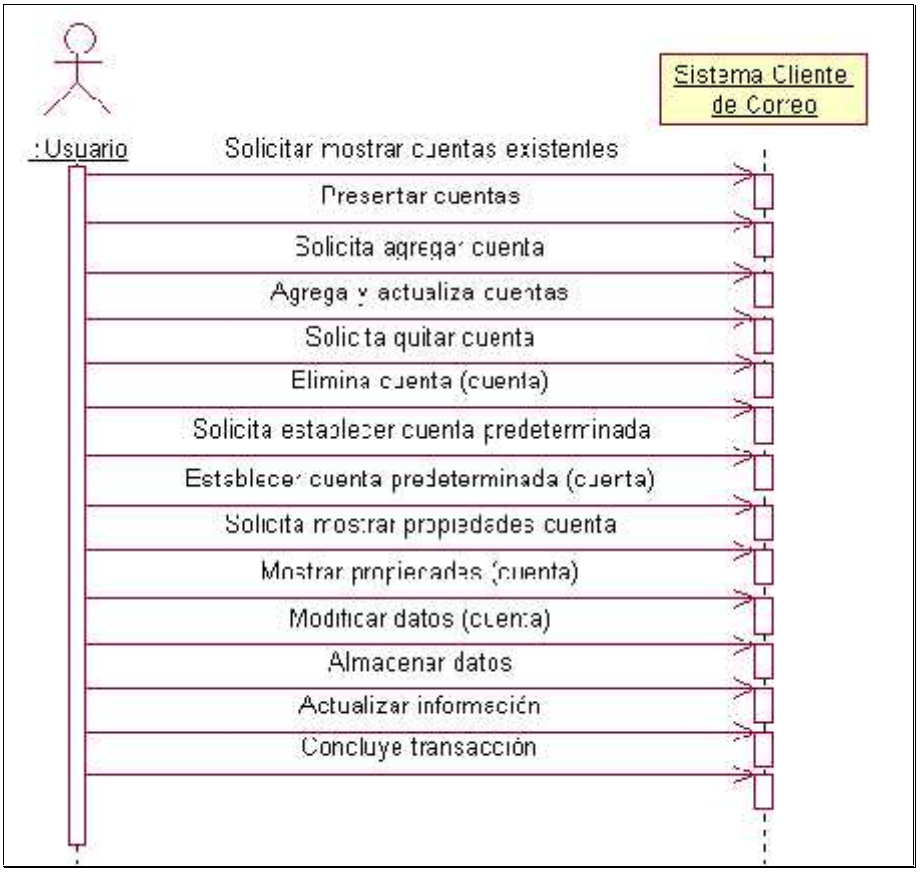


Figura # 6.12 Diagrama de Secuencia 03 (Caso de Uso CU_03)

Diagrama de Secuencia 04:

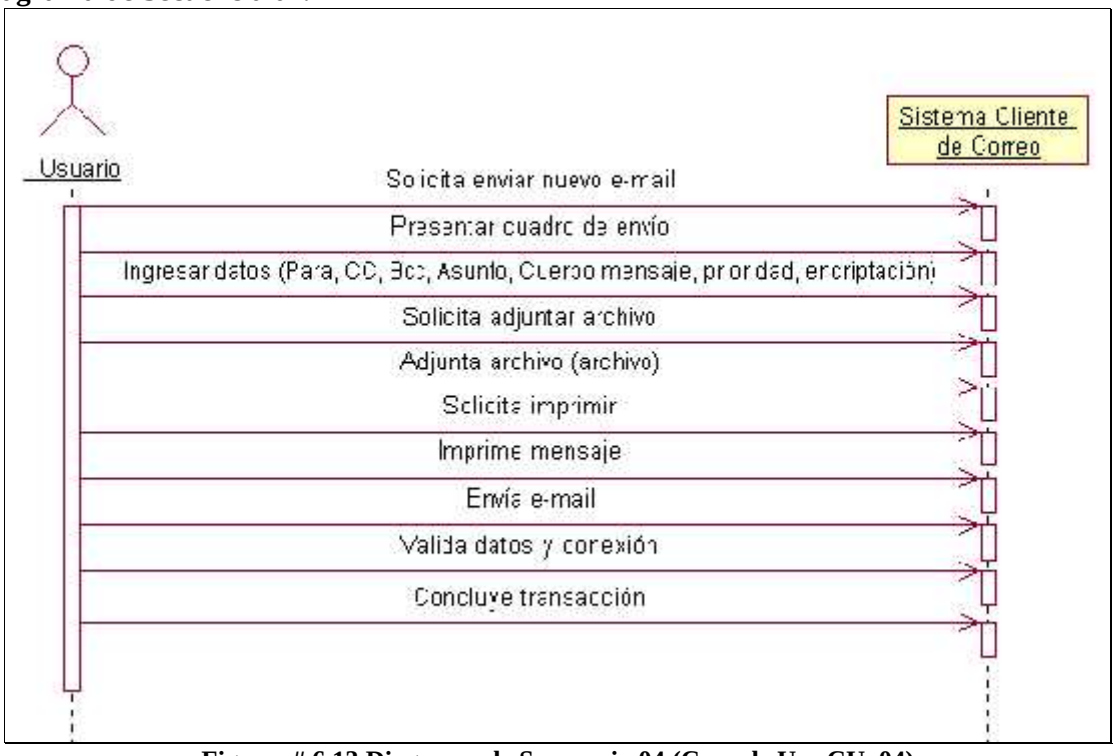


Figura # 6.13 Diagrama de Secuencia 04 (Caso de Uso CU_04)

Diagrama de Secuencia 05:

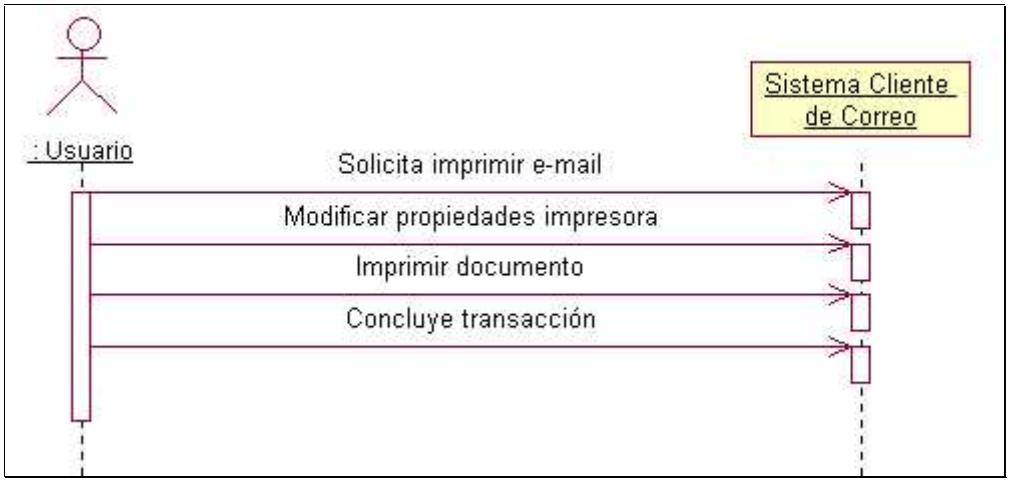


Figura # 6.14 Diagrama de Secuencia 05 (Caso de Uso CU_05)

Diagrama de Secuencia 06:

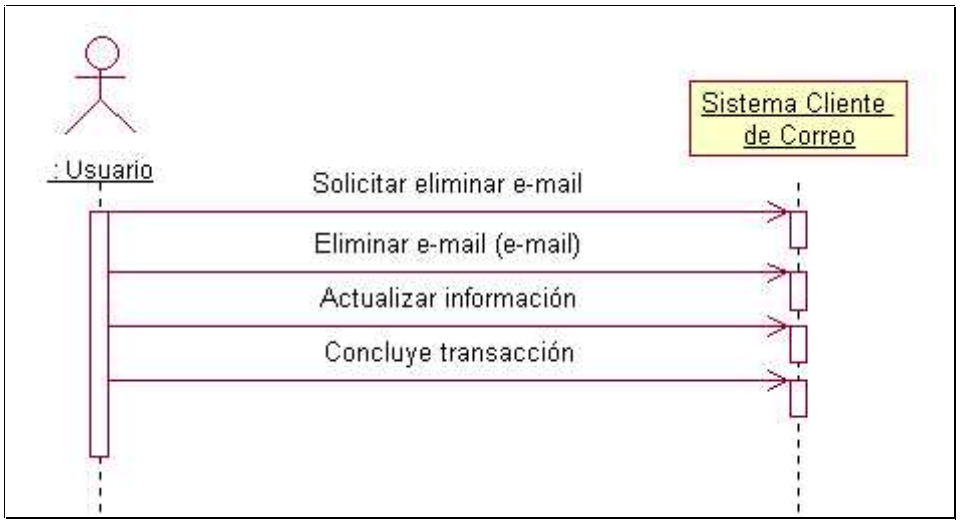


Figura # 6.15 Diagrama de Secuencia 06 (Caso de Uso CU_06)

Diagrama de Secuencia 08:

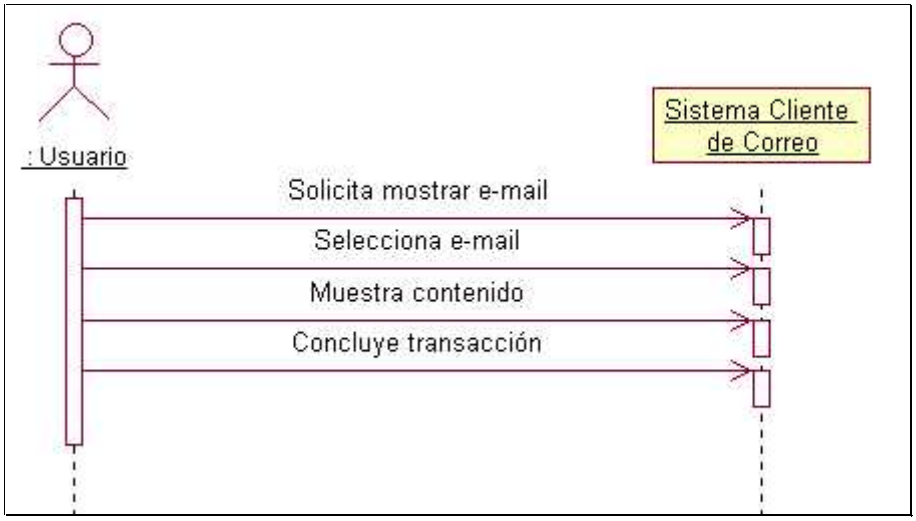


Figura # 6.16 Diagrama de Secuencia 08 (caso de Uso CU_08)

Diagrama de Secuencia 09:

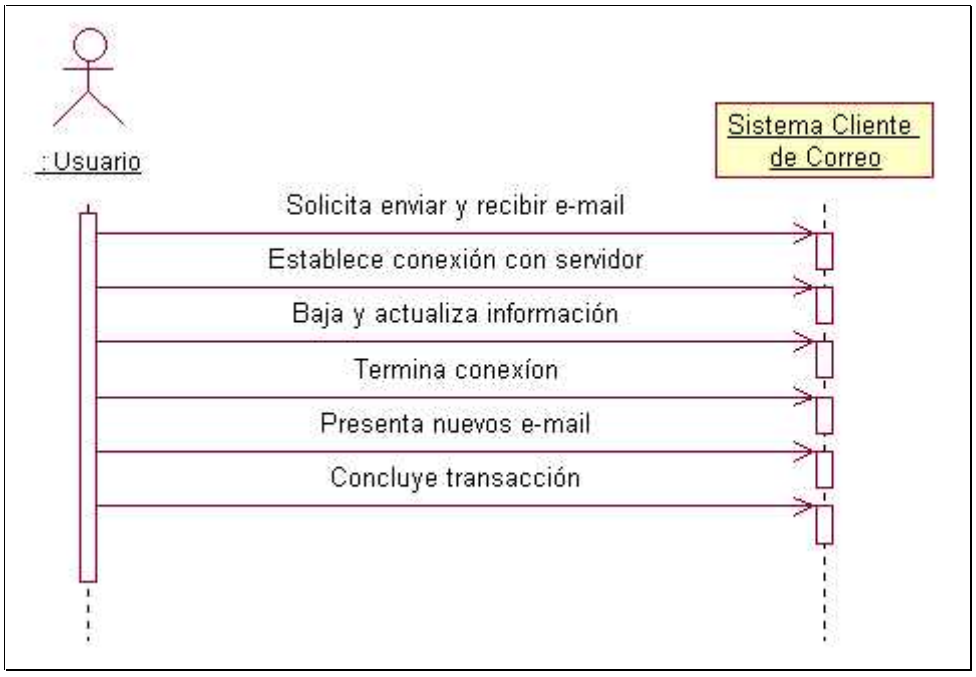


Figura # 6.17 Diagrama de Secuencia 09 (caso de Uso CU_09)

Diagrama de Secuencia 10:

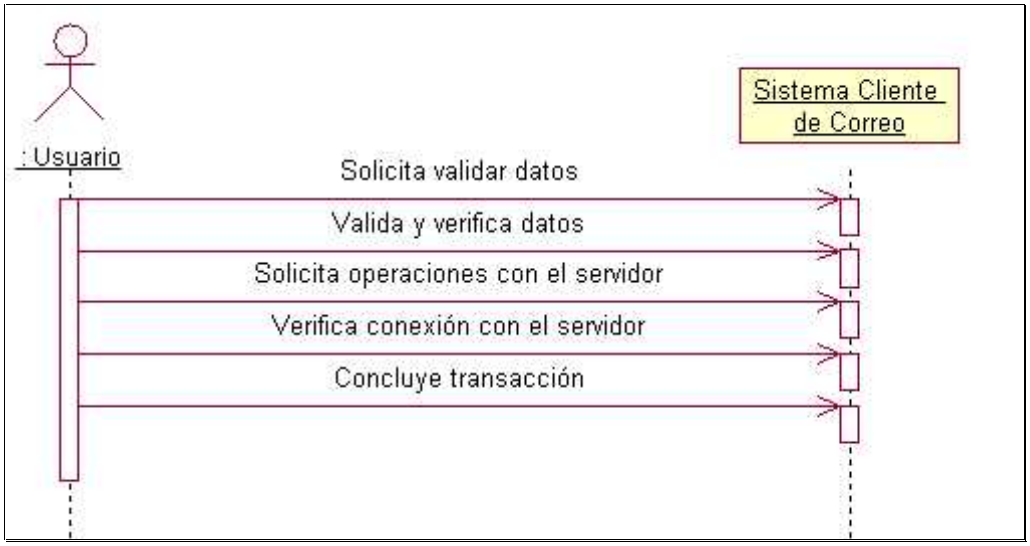


Figura # 6.18 Diagrama de Secuencia 10 (caso de Uso CU_10)

6.5 DICCIONARIO DE OBJETOS

El diccionario de objetos es una descripción general de los actores o entidades que intervienen en el manejo del sistema, además especifica las relaciones existentes entre estos, así como los atributos y operaciones que realizan mediante la utilización del sistema informático

Término	Categoría	Descripción
Crear o agregar nueva cuenta	Caso de uso	Crear o agregar una nueva cuenta de correo electrónico.
Operaciones con cuentas	Caso de uso	De una lista de cuentas creadas permitir al usuario agregar, quitar establecer como predeterminada una cuenta o cambiar las propiedades de una cuenta en particular.
Enviar nuevo e-mail	Caso de uso	El usuario crea un nuevo e-mail, para luego enviarlo a un destinatario en particular.
Imprimir e-mail	Caso de uso	Imprimir mediante el sistema, un e-mail cualquiera de las carpetas locales.
Eliminar e-mail	Caso de uso	Elimina mediante el sistema, un e-mail cualquiera de las carpetas locales.
Agregar nueva dirección	Caso de uso	Agregar una nueva dirección de correo electrónico para definir una lista de contactos.
Mostrar e-mail	Caso de uso	Permite mostrar la información que contiene un e-mail independientemente de donde se ubique (Bandeja de entrada, Bandeja de salida, Elementos enviados, Elementos eliminados, Borrador).
Enviar y recibir e-mail	Caso de uso	Similar a una actualización general de toda la información de las carpetas locales.

Manejo de errores	Caso de uso	Se encarga de validar y verificar antes de cada operación para indicar si existen errores en el proceso mediante mensajes de error. El manejo de errores no solo se refiere a errores de sintaxis como no escribir correctamente el nombre del destinatario, sino que además también está encargado de los errores de conexión.

Tabla # 6.9 Diccionario de Objetos

6.6 CONTRATO DE OPERACION

Los contratos de operación son documentos que describen la responsabilidad de una operación dentro del sistema, de esta manera se espera tener un control adecuado de los parámetros antes y después de una determinada acción. Se puede describir un contrato para un método individual o para una operación del sistema completo.

Para el sistema Cliente de Correo se ha tomado en cuenta las siguientes operaciones como las más importantes en la ejecución del mismo.

Contrato de Operación 1

Nombre	Codificar
Responsabilidades	Utilizar una cuenta activa para realizar esta operación, la misma que se encargara de garantizar la integridad de los datos y brindar seguridad de alto nivel.
Referencia cruzadas	CU_03
Excepciones	Opción de “sin encriptación”
Notas	Si al enviar un nuevo e-mail, se ha escogido la opción de “sin encriptación”
Pre-condiciones	El Usuario emisor llena todos los datos necesarios para enviar un e-mail encriptado.
Post-condiciones	El e-mail ha sido encriptado y solo podrá ser abierto por el usuario receptor quién también cuente con el sistema Cliente de Correo y ha iniciado su respectiva cuenta.

Tabla # 6.10 Contrato de Operación 1 - Codificar

Contrato de Operación 2

Nombre	Mostrar cuentas
Responsabilidades	Mostrar todas las cuentas existentes que se han creado o agregado a la lista de cuentas, además permitir al usuario visualizar cual es la cuenta predeterminada.
Referencia cruzadas	CU_02
Excepciones	Lista de cuentas vacía.
Notas	Si se utiliza por primera vez el sistema o se han eliminados todas las cuentas anteriormente.
Pre-condiciones	El usuario ha iniciado una cuenta activa y solicita ver todas las cuentas existentes.
Post-condiciones	Se muestran todas las cuentas existentes en el sistema, cada una con su tipo (predeterminada o no) y conexión.

Tabla # 6.11 Contrato de Operación 2 – Mostrar cuentas

Contrato de Operación 3

Nombre	Mostrar propiedades de cuenta seleccionada.
Responsabilidades	El sistema almacena un tipo de configuración por cada cuenta, el mismo que puede ser modificado si así lo desea el usuario.
Referencia cruzadas	CU_02
Excepciones	No existen.
Notas	
Pre-condiciones	Luego que el usuario haya iniciado una cuenta activa debe seleccionar una cuenta para ver sus propiedades.
Post-condiciones	Se muestra un cuadro de diálogo con las propiedades de la cuenta dividida en tres fichas (General, Servidores y Opciones Avanzadas).

Tabla # 6.12 Contrato de Operación 3 – Mostrar propiedades de cuenta seleccionada

Contrato de Operación 4

Nombre	Quitar cuenta seleccionada.
Responsabilidades	Eliminar la cuenta seleccionada del sistema.
Referencia cruzadas	CU_02
Excepciones	No existen.
Notas	
Pre-condiciones	Se ha iniciado una cuenta activa y el usuario selecciona una cuenta en particular para ser eliminada.
Post-condiciones	La cuenta es eliminada satisfactoriamente y desaparece de la lista de cuentas.

Tabla # 6.13 Contrato de Operación 4 – Quitar cuenta seleccionada

Contrato de Operación 5

Nombre	Establecer como cuenta predeterminada.
Responsabilidades	Fijar solo una cuenta a la vez como predeterminada, no se pueden establecer dos o más cuentas predeterminadas, solo una.
Referencia cruzadas	CU_02
Excepciones	Lista de cuentas vacía.
Notas	Si no existen cuentas creadas o agregadas, no es posible fijar como predeterminada, ya que no hay manera de seleccionar una cuenta en particular.
Pre-condiciones	Dentro de una cuenta activa seleccionar una cuenta en particular para establecer como predeterminada.
Post-condiciones	La cuenta que ha sido seleccionada quedará establecida como predeterminada.

Tabla # 6.14 Contrato de Operación 5 – Establecer como cuenta predeterminada

Contrato de Operación 6

Nombre	Guardar la configuración de cuentas.
Responsabilidades	Guardar las modificaciones que se han realizado en una cuenta ya creada o almacenar las propiedades de una nueva cuenta.
Referencia cruzadas	CU_02
Excepciones	No existen.
Notas	
Pre-condiciones	En una cuenta activa el usuario desea crear una nueva cuenta o modificar una existente.
Post-condiciones	Almacenar los datos de una nueva cuenta, y las modificaciones en una cuenta existente.

Tabla # 6.15 Contrato de Operación 6 – Guardar la configuración de cuentas

Contrato de Operación 9

Nombre	Leer correo.
Responsabilidades	Mostrar el contenido de un correo en particular.
Referencia cruzadas	CU_07
Excepciones	Carencia de correos.
Notas	No existen correos para ver su contenido.
Pre-condiciones	En una cuenta activa el usuario elige leer un correo en particular.
Post-condiciones	El usuario puede ver el contenido de su e-mail, y si desea responderlo o reenviarlo.

Tabla # 6.16 Contrato de Operación 9 – Leer correo

Contrato de Operación 10

Nombre	Enviar e-mail.
Responsabilidades	Realizar todas las operaciones, validaciones y verificaciones necesarias tanto en la sintaxis como en la conexión antes de enviar un nuevo e-mail.
Referencia cruzadas	CU_03, CU_04
Excepciones	Errores al enviar.
Notas	Pueden ser errores de sintaxis como escribir mal la cuenta de destino o errores de conexión con el servidor.
Pre-condiciones	En una cuenta activa el usuario desea enviar un nuevo e-mail, para lo que se encarga de llenar todos los datos necesarios para dicha operación.
Post-condiciones	No existieron errores y el e-mail se envió satisfactoriamente a su destinatario.

Tabla # 6.17 Contrato de Operación 10 – Enviar e-mail

Contrato de Operación 11

Nombre	Eliminar e-mail.
Responsabilidades	Realizar la conexión con el servidor y eliminar el mensaje seleccionado.
Referencia cruzadas	CU_05
Excepciones	Error de conexión.
Notas	Si la conexión con el servidor ha fallado, no será posible eliminar el mensaje en cuestión.
Pre-condiciones	En una cuenta activa el usuario desea eliminar un e-mail en particular.
Post-condiciones	No existieron errores de conexión y el e-mail seleccionado ha sido eliminado satisfactoriamente.

Tabla # 6.18 Contrato de Operación 11 – Eliminar e-mail

Contrato de Operación 12

Nombre	Enviar y recibir.
Responsabilidades	Realizar una conexión con el servidor y mostrar los nuevos mensajes si los hay, caso contrario presentar un mensaje que indique que no hay mensajes en el servidor. Luego se cerrará la conexión.
Referencia cruzadas	CU_08
Excepciones	Error de conexión.
Notas	Si la conexión con el servidor ha fallado, no será posible actualizar la nueva información.
Pre-condiciones	En una cuenta activa el usuario solicita actualizar su información para ver sus nuevos mensajes.
Post-condiciones	No existieron errores de conexión y el usuario puede ver sus nuevos mensajes.

Tabla # 6.19 Contrato de Operación 12 – Enviar y recibir

6.7 DIAGRAMA DE ESTADOS

Tomando en cuenta un estado como un modo observable de comportamiento del sistema, se ha querido captar este comportamiento, para de una forma más clara describir los sucesos y transiciones que hacen que el sistema cambie de estado.

Un diagrama de transición de estados indica como se mueve el sistema de un estado a otro permitiéndole al desarrollador comprender que acciones se llevan a cabo como consecuencia de un suceso determinado.

El diagrama de estado que se describe a continuación representa de una forma general el comportamiento del sistema Cliente de Correo.

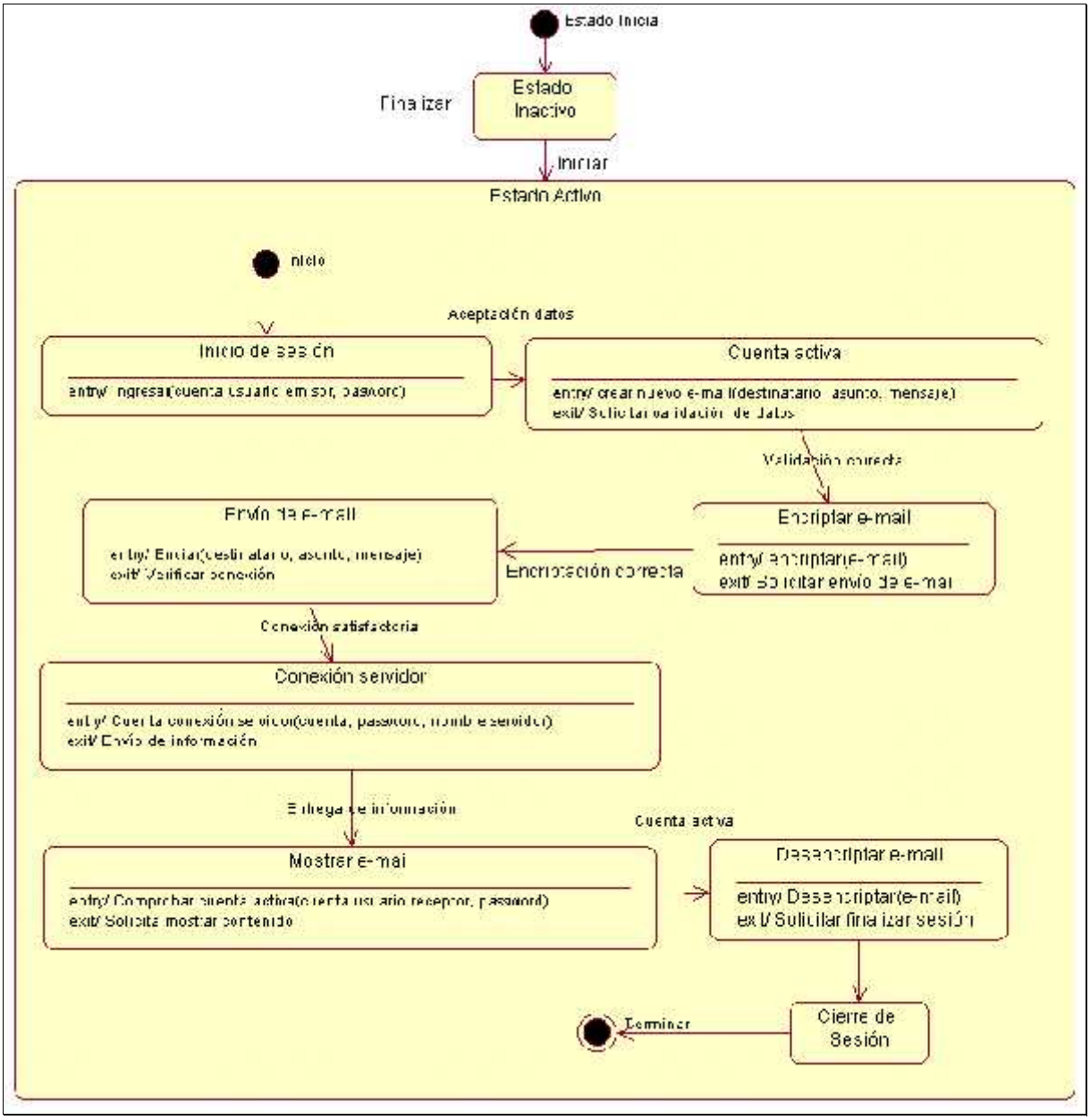


Figura # 6.19 Diagrama de Estados

6.8 DIAGRAMA DE CALLES

Este diagrama está fundamentalmente destinado para indicar la funcionalidad del sistema y el hecho de definirlo y refinarlo es la finalización de la fase del análisis. Cuando el diagrama de calles está terminado podemos dar paso al diseño.

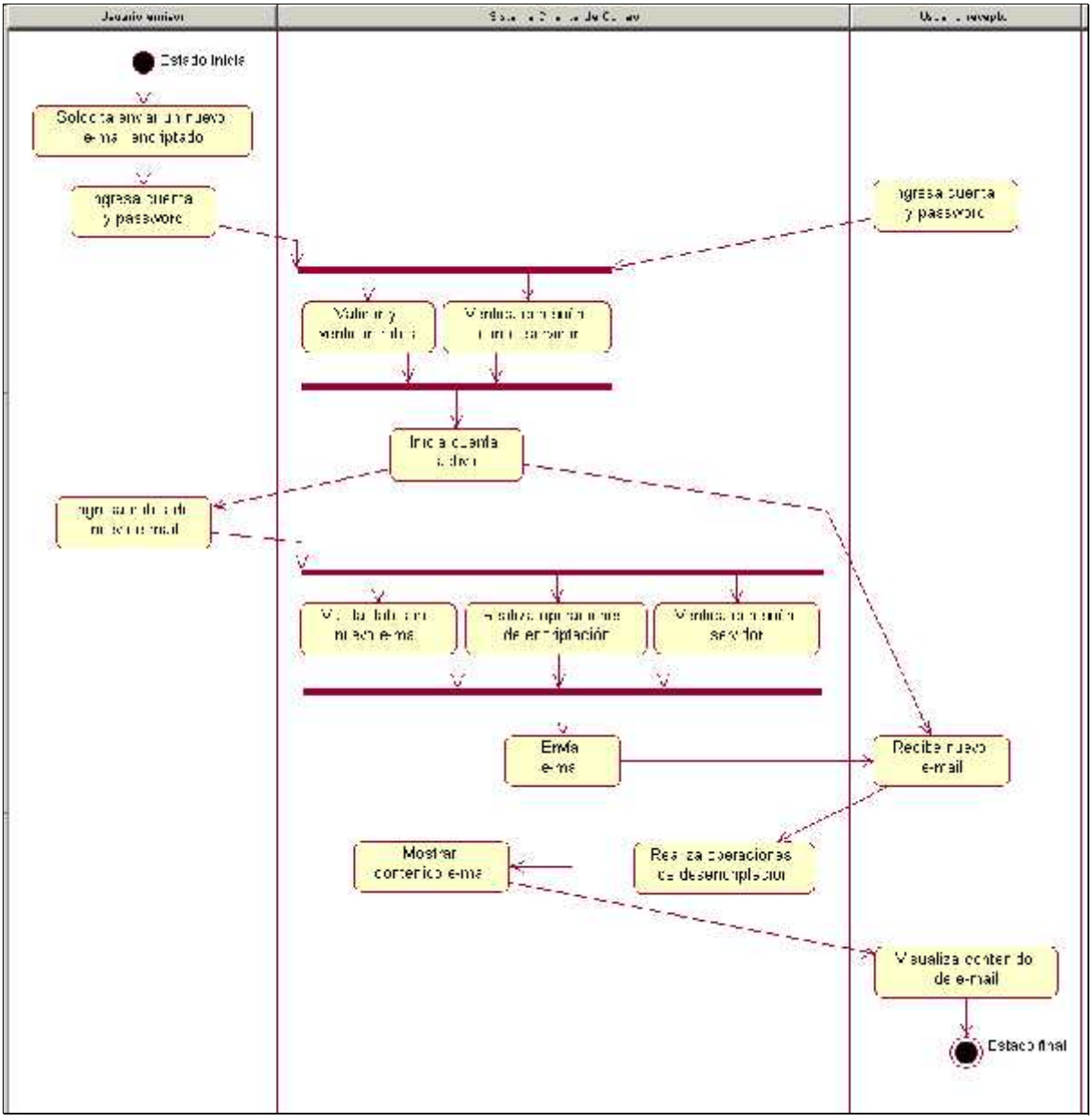


Figura # 6.20 Diagrama de Calles

6.9 DIAGRAMAS DE COLABORACION

Diagrama de Colaboración 01:

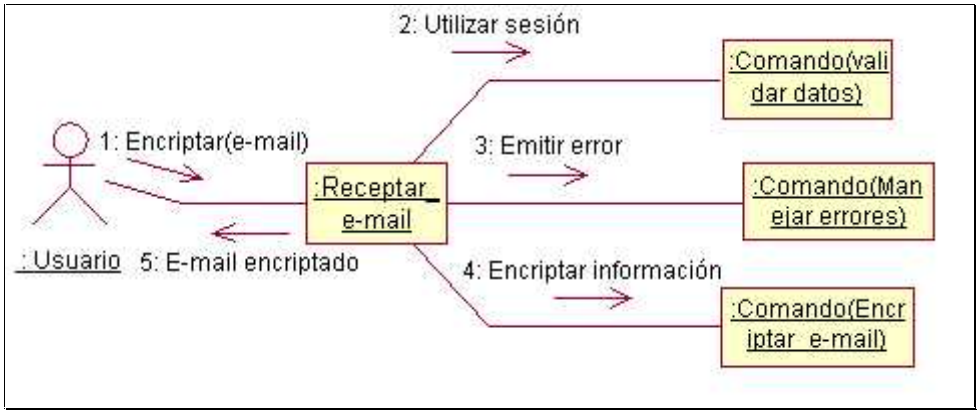


Figura # 6.21 Diagrama de Colaboración - Codificación

Diagrama de Colaboración 02:

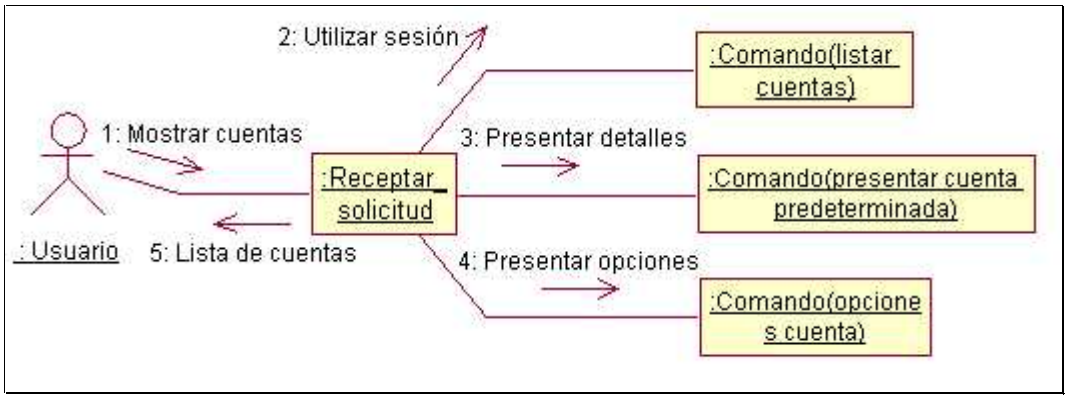


Figura # 6.22 Diagrama de Colaboración- Mostrar Cuenta

Diagrama de Colaboración 03:

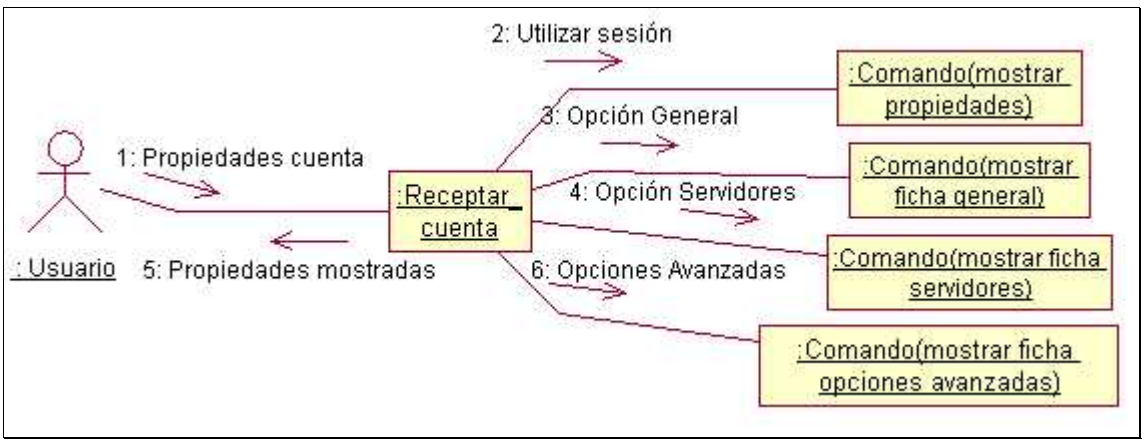


Figura # 6.23 Diagrama de Colaboración- Mostrar Propiedades de la Cuenta

Diagrama de Colaboración 04:

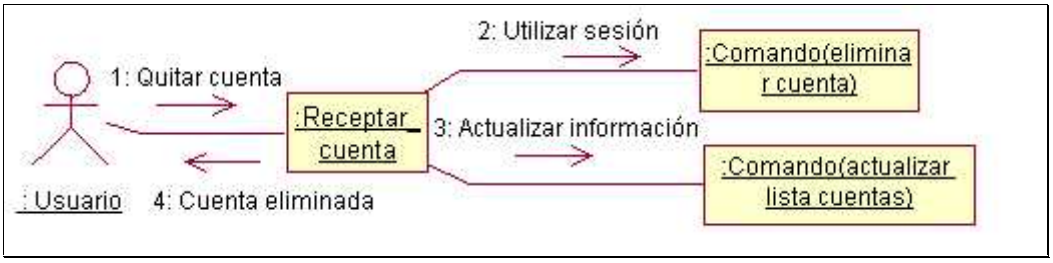


Figura # 6.24 Diagrama de Colaboración – Quitar cuenta seleccionada

Diagrama de Colaboración 05:

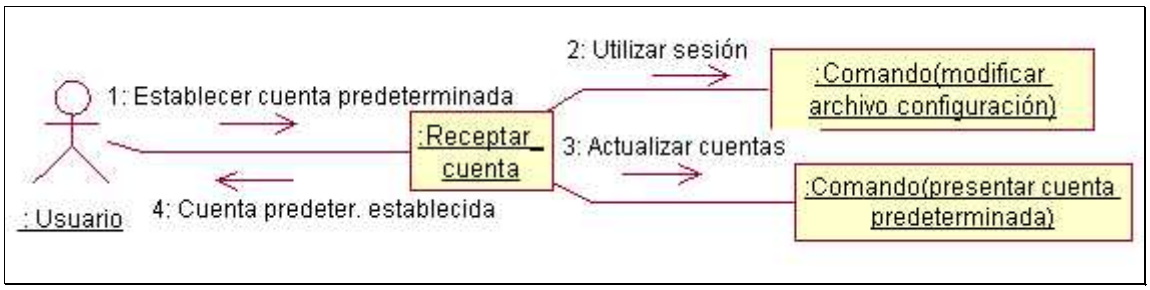


Figura # 6.25 Diagrama de Colaboración – Establecer cuenta predeterminada

Diagrama de Colaboración 06:

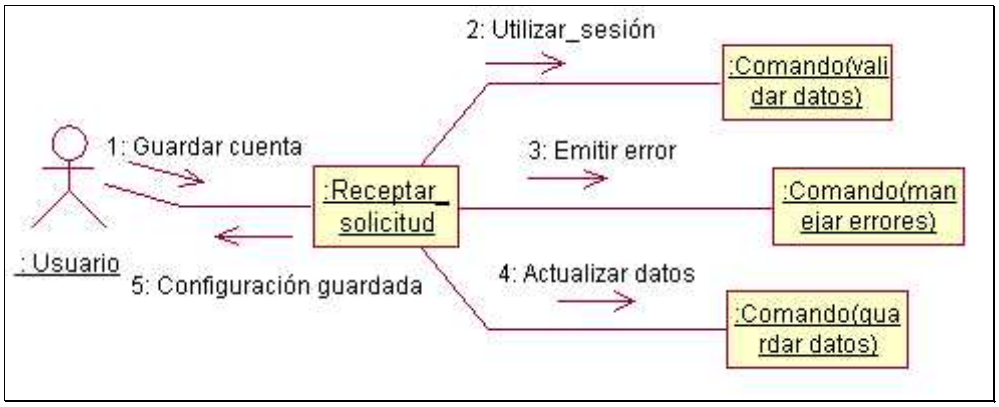


Figura # 6.26 Diagrama de Colaboración – Guardar cuenta

Diagrama de Colaboración 09:

Figura # 6.27 Diagrama de Colaboración – Leer un e-mail

Diagrama de Colaboración 10:

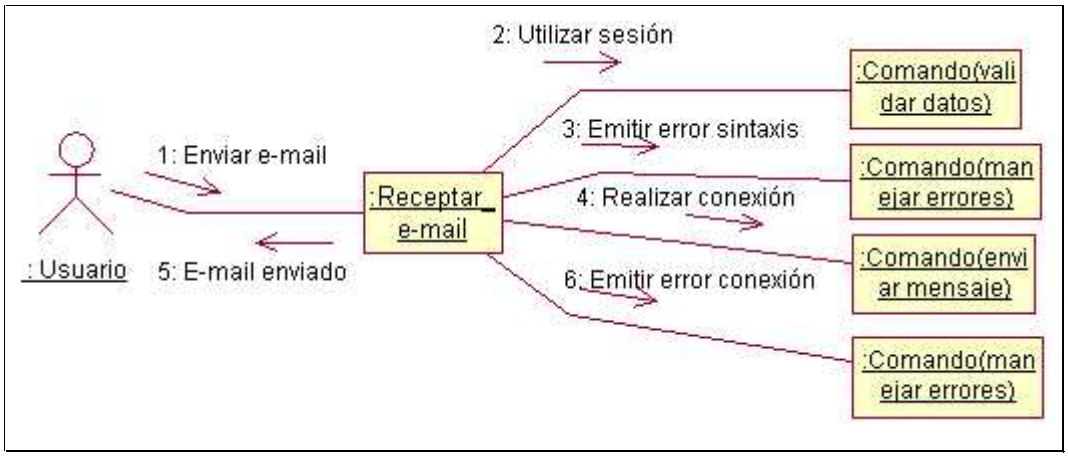


Figura # 6.28 Diagrama de Colaboración – Enviar un e-mail

Diagrama de Colaboración 11:

Figura # 6.29 Diagrama de Colaboración – Quitar un e-mail

Diagrama de Colaboración 12:

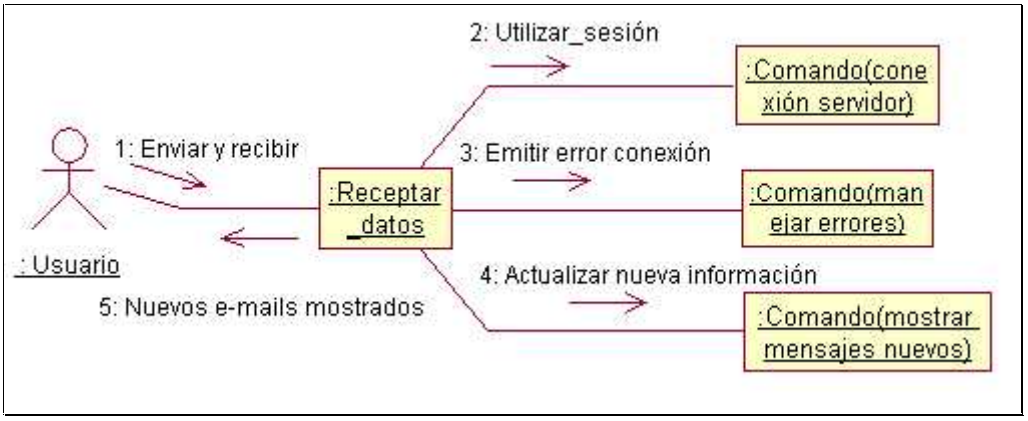


Figura # 6.30 Diagrama de Colaboración – Enviar y recibir un e-mail

6.10 REFINAR EL MODELO FISICO Y LA ARQUITECTURA DEL SISTEMA

En esta parte modelaremos los aspectos físicos del sistema orientado a objetos, teniendo en cuenta tanto los componentes que pertenecen al mundo físico como los respectivos al mundo virtual de software.

6.10.1 DIAGRAMA DE COMPONENTES

El Diagrama de Componentes describe el comportamiento de las clases en el sistema.

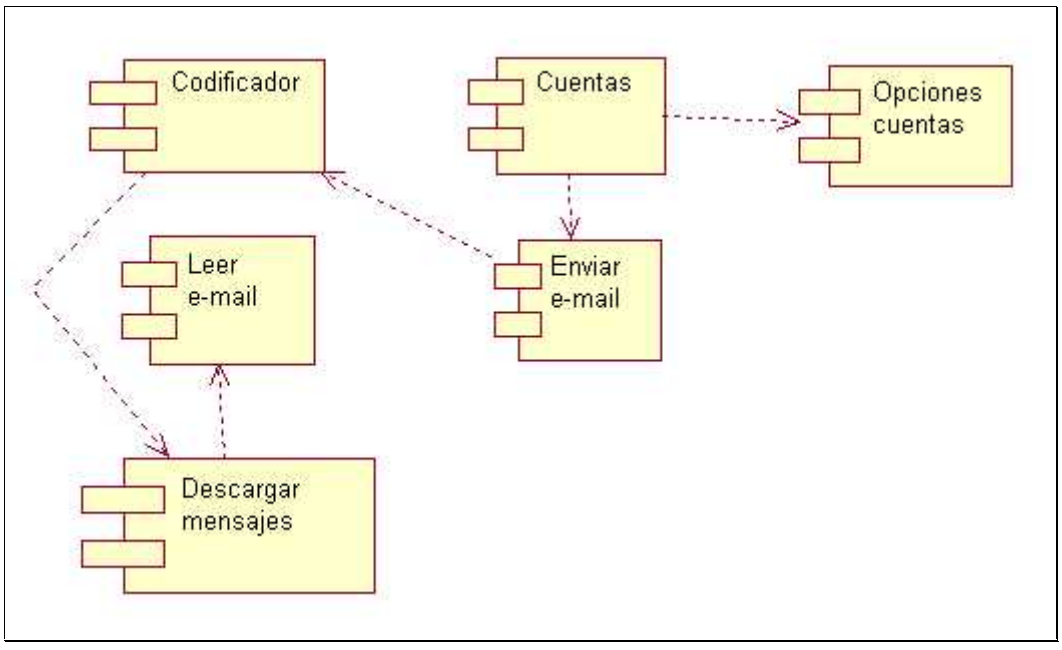


Figura # 6.31 Diagrama de Componentes

6.10.2 DIAGRAMA DE DESPLIEGUE

En este diagrama se representa tanto los componentes hardware como software que requiere este sistema para funcionar correctamente.

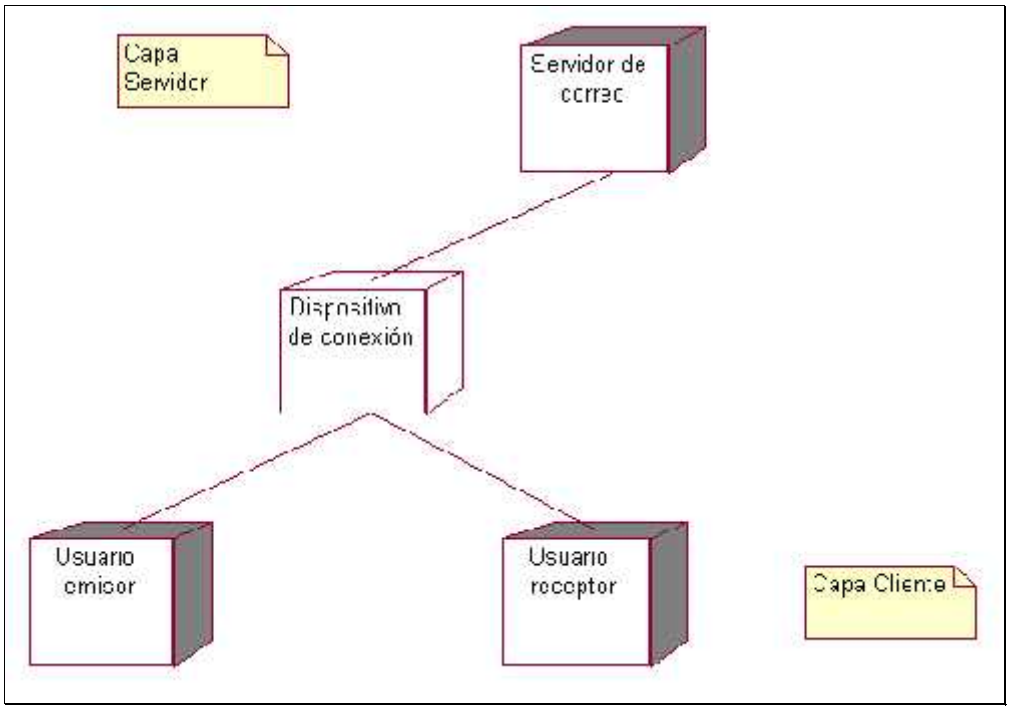


Figura # 6.32 Diagrama de Despliegue

CONCLUSIONES Y RECOMENDACIONES

CONCLUSIONES

- La seguridad en la transmisión y recepción de mensajes de correo electrónico se fortalecerá un 28% al utilizar el Cliente de Correo *Propuesto*, y el método de encriptación usado en el Administrador de Correo es un 47% alternativo en relación a otros mecanismos de encriptación.
- Para enviar y recibir mensajes encriptados, la mayor parte de Clientes de Correo Electrónico utilizan un identificador digital de una entidad emisora de certificados, lo cual implica un proceso de solicitud, aceptación y envío (por un período corto de tiempo) de un certificado, tanto para el emisor como para los destinatarios. Con lo que la *Propuesta* planteada en la presente investigación evita todo este proceso engorroso.
- La seguridad de un sistema de encriptación depende fundamentalmente del secreto que las claves tengan, es por eso, que se ha dado una real importancia en la gestión de las claves y el algorimo de encriptación para proponer un método de encriptación dinámico.
- Al ser el correo electrónico uno de los sistemas telemáticos más vulnerables a los ataques de seguridad, se ha diseñado un manera de mantener oculta la información para que sea accesible

únicamente por los usuarios autorizados es decir aquellos que utilicen el Cliente de Correo *Propuesto*.

- El funcionamiento de correo electrónico ha quedado normado por estándares como SMTP, POP3, MIME, etc. los cuales facilitan solamente la interacción. Partiendo de esto, se ha considerado el desarrollo de un mecanismo de encriptar los mensajes de correo electrónico, para mantener la seguridad en la transmisión de e-mail.
- Se considera que el método propuesto resalta el encubrimiento de la clave mediante la confusión y difusión, siendo un proceso muy estratégico para evitar criptoanálisis estadístico.
- A grandes rasgos se puede afirmar que en la criptografía simétrica, es posible conseguir mayores velocidades en relación a la criptografía asimétrica. Y además se debe considerar que la criptografía asimétrica ayuda a resolver el problema de la gestión de claves, aunque esté cuestionada la certificación de las claves públicas.
- La aleatoriedad de las claves, dificulta la recordación de las mismas, y la elección de una clave propia se entra en riesgo de escoger las mismas claves y en general se facilita realizar criptoanálisis con mucho texto cifrado y con la misma clave. Razón por la cual se pensó en la variabilidad o dinamismo en la generación de las claves que a su vez provoca la variabilidad o dinamismo en el criptosistema.
- El algoritmo IDEA se ha convertido en uno de los cifrados de bloque más populares debido a que es bastante seguro, ha resistido numerosos ataques y además la longitud de clave usada, 128 imposibilita actualmente una búsqueda exhaustiva.
- El Cliente de Correo desarrollado como objetivo de la presente investigación gestiona la transmisión y recepción de mensajes encriptados, siendo transparente al interactuar con el usuario.

RECOMENDACIONES

- Utilizar Cliente de Correo *Propuesto* cuando se desee enviar y recibir mensajes de correo encriptados, sin necesidad de recurrir entidades emisoras de certificados. Opcionalmente se puede ejecutar el Cliente de Correo para enviar y recibir correos normalmente sin encriptarlos.
- Se sugiere analizar detenidamente la forma de seleccionar el algoritmo de encriptación y la forma de gestionar las claves, ya que la seguridad de un sistema de encriptación dependerá fundamentalmente de estos dos criterios.
- Profundizar el aprendizaje de estándares relacionados a la área de aplicación, de acuerdo al tipo de software que se desee desarrollar, para producir resultados satisfactorios y eficientes.
- Desarrollar aplicaciones de Correo Electrónico para el Web utilizando protocolos seguros, pero haciendo innatas las características de criptografía.
- Se recomienda aplicar técnicas criptográficas no solamente en el Correo Electrónico, sino también en otras áreas relacionadas como la Web, comunicaciones en Redes, desarrollo de aplicaciones de software, y otras propias de criptografía.
- Considerar que al utilizar el Cliente de Correo *Propuesto* en la presente investigación así como cualquier Cliente de Correo tradicional, se debe siempre primero configurar la cuenta o buzón para su normal desempeño.
- Se debe realizar ampliamente pruebas de funcionamiento de un software que se desarrolla en forma paulatina, ya que se descubre problemas y errores que aportan al mejoramiento del producto final.

GLOSARIO

Autenticación

En un sistema operativo de red o multiusuario, el proceso que valida la información de ingreso de un usuario. Por lo general, la autenticación involucra la comparación del nombre y las contraseñas con una lista de usuarios autorizados; si hay coincidencia, el usuario puede ingresar al sistema de acuerdo con los derechos o permisos asignados a su cuenta.

Autenticidad

Se refiere a estar seguros de la identidad de una entidad ya sea mensaje, persona, servidor etc.

Autoridad certificadora: es una entidad (compañía) que es reconocida para poder certificar la asociación de una clave pública a una persona o servidor.

Certificado Digital

Físicamente es un archivo de hasta 2K de tamaño que contiene principalmente, los datos de una entidad una persona o un servidor, la clave pública de esa entidad, y la firma de una autoridad certificadora que es reconocida con la capacidad de poder comprobar la identidad de la persona (o servidor) y válida la clave pública que es asociada a la entidad.

Cifrador de Bloque**: es un sistema criptográfico que cifra de bloques en bloque, usualmente cada bloque es de 128 bits. Algunos sistemas conocido son, TDES, RC5, AES.**

Cifrador de Flujo: es un sistema criptográfico de cifra de bit en bit, los más conocidos son, RC4, SEAL, WAKE.

Cifrar

Es la acción que produce un texto cifrado (Ilegible) a partir de un texto original

Clave Privada

Es la clave secreta que se usa en la criptografía asimétrica

Clave Pública

Es la clave públicamente conocida, que se usa en la criptografía asimétrica

Clave Simétrica

Es la clave secreta que tienen ambos lados de una comunicación en la criptografía simétrica.

Compartición de secretos

Es un esquema criptográfico que tiene como entrada un secreto (por ejemplo una clave criptográfica) y como salida un numero *n* de partes del secreto y todas o algunas de éstas *n* partes sirven para reconstruir el secreto.

Correo Electrónico (E-Mail)

Correo enviado a través de medios electrónicos. Aunque originalmente se trataba de mensajes de texto, actualmente puede cualquier otro tipo de información.

Criptografía

Es el conjunto de técnicas (entre algoritmos y métodos matemáticos) que resuelven los problemas de autenticidad, privacidad, integridad y no rechazo en la transmisión de la información.

Criptografía Asimétrica

Es el conjunto de métodos que permite establecer comunicación cifrada, donde una de las claves es pública y la otra clave es privada (secreta). Cada usuario tiene un par de claves una pública y otra privada.

Criptografía Simétrica

Es el conjunto de métodos que permite establecer comunicación cifrada, con la propiedad de que ambos lados de la comunicación tienen la misma clave, y ésta es secreta.

Cuenta Dial-Up (Marcación Directa)

Cuenta de Internet que permite la conexión vía modem a la red. Normalmente requiere de la contratación con un ISP (Internet Service Provider, Proveedor de Servicios de Internet) quien cuenta con una conexión dedicada a la red y revende el acceso a través de bancos de módems.

Cuenta de Usuario

Acceso para un usuario a una máquina Servidor de Correo. Cada cuenta de usuario tiene un único nombre de usuario e ID de seguridad

Descifrar

Es la acción inversa de cifrar, es decir, convierte un texto cifrado a otro legible (texto original)

Dirección

Código con el que Internet identifica a un usuario específico. Su formato es:
Nombre_de_usuario@nombre deservidor, donde *nombre_de_usuario*, es el nombre del usuario, nombre de acceso o número de cuenta y *nombre_de_servidor*, es el nombre de la computadora o proveedor de Internet que se está utilizando. Un nombre de servidor puede contar de varias palabras separadas por puntos.

Dirección IP

Conjunto único de cuatro números separados por puntos (por ejemplo: 165.113.245.2), que identifica a una máquina dentro de Internet. Todas las máquinas de Internet tiene un único número IP.

Encriptación

Conjunto de técnicas que intentan hacer inaccesible la información a personas no autorizadas. Por lo general, la encriptación se basa en una clave, sin la cual la información no puede ser descifrada. Se puede hablar de dos sistemas de encriptación: sistemas simétricos, en los que se utiliza la misma clave para cifrar y descifrar el mensaje, y sistemas asimétricos, en los que se utiliza una clave para cifrar el mensaje y otra distinta para descifrarlo.

Esquema criptográfico: es un conjunto de primitivas que componen una aplicación criptográfica más completa, como el esquema de firma digital (compuesta de la primitiva de firma y la de verificación), el esquema de cifrado (compuesta con la primitiva de cifrado y la de descifrado) etc.

Familia criptográfica

Es el conjunto de sistemas criptográficos que basan su seguridad en el mismo problema matemático, actualmente las familias criptográficas más conocidas son las que basan su seguridad en el Problema de Factorización Entera (RSA, RW), los que la basan en el problema del logaritmo discreto (DH, DSA), y los que la basan en el problema del logaritmo discreto elíptico (DHE, DSAE, MQV)

Firma digital

Es un método que usa la criptografía asimétrica y permite autenticar una entidad (persona o servidor), tiene una función igual que la firma convencional. Consiste en dos procesos, uno de firma y otro de verificación de la firma. Físicamente es una cadena de caracteres que se adjunta al documento.

Función hash: es una función de un solo sentido, resistente a colisiones que asocia un archivo o documento de longitud arbitraria a una cadena de longitud constante (se usa actualmente 160b de salida), las funciones hash más conocidas son: MD5, SHA1, RIPMED 160.

Generador de números seudoaleatorios: es una función que tiene como entrada una cadena (conjunto de bits) llamada semilla y como salida otra cadena de bits que al aplicarle ciertas pruebas de aleatoriedad pasan con un porcentaje aceptable (alrededor de un 95%)

Host

Dispositivo dentro de una red que utiliza TCP/IP.

Inicio de Sesión.

Identificarse uno mismo ante la computadora.

Integridad

Se refiere a que la información no sea modificada

Internet

Conjunto de Interconexiones formado por todas las redes del mundo que utilizan TCP/IP.

Intranet

Red con una organización específica que conecta computadoras entre sí.

Longitud de la clave

Es el número de bits (ceros y unos) que tienen las claves y es solo uno de los parámetros de los que depende la seguridad de un sistema criptográfico. Actualmente se usan 128 para las claves simétricas, 1024 para el sistema asimétrico RSA, 163 para los sistemas asimétricos que usan curvas elípticas.

No-rechazo

Se refiere a no poder negar la autoría de un mensaje o de una transacción.

Par de claves

Se refiere al par de claves una privada y otra pública usadas en la criptografía asimétrica.

Primitiva criptográfica: es la función más básica que compone un sistema criptográfico, existen la primitiva de cifrado, la primitiva de descifrado, la primitiva de firma, la primitiva de verificación de firma etc.

Privacidad

Se refiere a tener control en el acceso de la información y solo permitirlo a personas autorizadas

POP (Post Office Protocol; Protocolo De Oficina Postal)

Protocolo empleado por el software cliente para extraer mensajes de los servidores de correo.

Protocolo (criptográfico): es la parte más visible de la aplicación y esta compuesto de esquemas criptográficos conjuntamente con otras operaciones que permiten proporcionar seguridad a una aplicación más específica, por ejemplo el protocolo SSL, SET, SMIME, IPsec etc.

Protocolo de Control de Transmisión/ Protocolo Internet (TCP/IP)

Protocolo que utilizan las redes para comunicarse con cualquier otra red dentro de Internet.

Protocolo Internet (IP)

Protocolo de transporte que forma una de las bases de Internet. IP permite dividir los datos en paquetes discretos de información, para ser transmitidos de una red a otra, siendo la red de destino la encargada de ensamblarlos de nuevo.

Servidor.

Computadora que provee de un servicio a otras computadoras dentro de la red. Un servidor de archivos por ejemplo, provee de archivos a todas las computadoras clientes.

SMTP (Simple Mail Transfer Protocol; Protocolo Sencillo De Transferencia De Correo)
Protocolo original para intercambio de correo en Internet. Sólo permite el intercambio de mensajes ASCII, por lo que está siendo gradualmente reemplazado por MIME.

Solicitudes de Comentarios (RFC)
Documentos que proveen de un método para que un diverso grupo de personas (los usuarios de Internet) puedan comunicarse y ponerse de acuerdo dentro de la arquitectura y funcionalidad de Internet. Algunos RFC son documentos oficiales del Internet Engineering Task Force (IEFC), el cual define los estándares de TCP/IP dentro de Internet; otros RFC se proponen como nuevos estándares de documento dentro de algún campo específico (unos de naturaleza tutorial, otros de naturaleza técnica).

TCP/IP (Transmission Control Protocol/Internet Protocol; Protocolo De Control De Transmision/Protocolo Internet)
Protocolos utilizados para la comunicación entre todos lo dispositivos de Internet. Fueron diseñados inicialmente para ambientes Unix por Vinton G. Cerf y Robert E. Kahn.

Texto cifrado
Es un documento que ha sido cifrado

Texto original
Es un documento antes de ser cifrado

ANEXOS

ANEXO No. 1

ENCUESTA SOBRE LA UTILIZACION DE SISTEMAS DE CORREO ELECTRÓNICO EN LA INTRANET DE LA ESPOCH

En el marco de ejecución del Proyecto "PROPUESTA DE UN METODO DE ENCRIPTACIÓN DE INFORMACIÓN EN LA TRANSMISIÓN DE CORREO ELECTRÓNICO EN LA INTRANET DE LA ESPOCH", presentado en la ESPOCH por el Ing. Danilo Pástor; se ha previsto la necesidad de realizar un diagnóstico y análisis en las principales usuarios de correo electrónico; la información recopilada nos permitirá conocer las tendencias actuales de seguridad en el marco de la transmisión de información a través del correo electrónico

La información proporcionada será utilizada con fines de investigación; el autor se hace responsable de la manipulación de los datos,

1. TIPO DE USUARIO

Permanente	☐	Otros (Especifique)	☐
Cotidiano	☐	.....	
Eventual	☐		
Poco común	☐		

2. SISTEMAS ADMINISTRADORES DE CORREO UTILIZADOS

2.1 Cuáles son los Administradores de correo electrónico que se usan en su empresa:

Outlook	☐	Fabricante/Versión:.....
Pegasus Mail	☐	Fabricante/Versión:.....
Elm	☐	Fabricante/Versión:.....
Netscape	☐	Fabricante/Versión:.....
Otros (especifique)	☐	
.....		Fabricante/Versión:.....

2.2 Cuales son los factores determinantes que conllevan a la utilización de un Sistema Administrador de correo específico?

Aspecto económico	☐	
Tendencias tecnológicas	☐	
Dependencia de una aplicación específica	☐	
Dependencia del hardware	☐	
Número de usuarios	☐	
Otros (especifique)	☐	.....

2.3 A su criterio: cuál(es) sistema(s) administrador de correo de los que actualmente utiliza es el más óptimo para el desempeño de sus actividades?

.....
Porqué? .....

2.4 Cuál es el número de correos diarios promedio que manipula usted
.....

3. TENDENCIAS FUTURAS

3.1 Planea su institución migrar a otros administradores de correo

SI ☐ NO ☐

Si su respuesta es afirmativa especifique a cual (es):
.....

3.2 A su criterio, cual es el aspecto que se debería considerar en un administrador de correo:

Seguridad ☐
Facilidad de manipulación ☐
Popular ☐

3.3 Existe en su institución seguridad en el manejo del correo electrónico:

SI ☐ NO ☐

Si su respuesta es afirmativa especifique entre cuales:
.....
.....

ANEXO No. 2

MANUAL DEL USUARIO
CLIENTE DE CORREO

1. INTRODUCCION

El manual del usuario de Cliente de Correo tiene como objetivo, proporcionar la información necesaria para facilitar el entendimiento de los procesos que conforman este software.

Este documento posee una descripción del manejo o gestión del CLIENTE DE CORREO, adicionalmente se han incluido las ventanas de entradas y salidas para una mejor comprensión de los procesos.

El manual está organizado en tres partes: Determinación de los requerimientos de hardware y Software, descripción general del sistema y una Descripción detallada del mismo.

2. REQUERIMIENTOS DE HARDWARE Y SOFTWARE

REQUERIMIENTOS DE HARDWARE

- Computadora Pentium 100 MHz en adelante
- 16 Mb RAM mínimo (se recomienda 32 Mb o más)

REQUERIMIENTOS DE SOFTWARE

- Sistema Operativo Windows 9X, Windows 2000, Windows XP

3. DESCRIPCION GENERAL

El prototipo de Cliente de Correo, es un software diseñado para trabajar con ambientes Windows y realiza las tareas más comunes y básicas de gestión de correo electrónico, implementada con el protocolo TCP/IP. Las funciones del Cliente de Correo son las siguientes:

- Gestión de cuentas de correo electrónico
- Gestión de creación de mensajes de correo electrónico
- Gestión de lectura de mensajes de correo electrónico
- Gestión de envío y recepción de correo electrónico
- Gestión de encriptación de correo electrónico

La aplicación *Cliente de Correo* esta organizada en tres grandes módulos:

- **Archivo**.- Se refiere al manejo de archivos nuevos y básicamente hace referencia a crear nuevos mensajes de correo electrónico.

- **Herramientas**.- Se refiere a la configuración de las cuentas y opciones de correo electrónico.

- **Mensaje**.- Se refiere a la gestión de mensajes; nuevos, eliminados, reenvió, etc.

- **Ayuda**.- Se refiere a la ayuda de sistema. Contiene los submódulos: Contenidos, Como usar la ayuda y Acerca de.

4. DESCRIPCION DETALLADA

Para la ejecución del sistema *Cliente de Correo* se debe hacer dobleclick en el icono con el mismo nombre ubicado en el escritorio de Windows XP.

Una vez que se ha ejecutado el sistema se presentará la pantalla inicial del sistema:

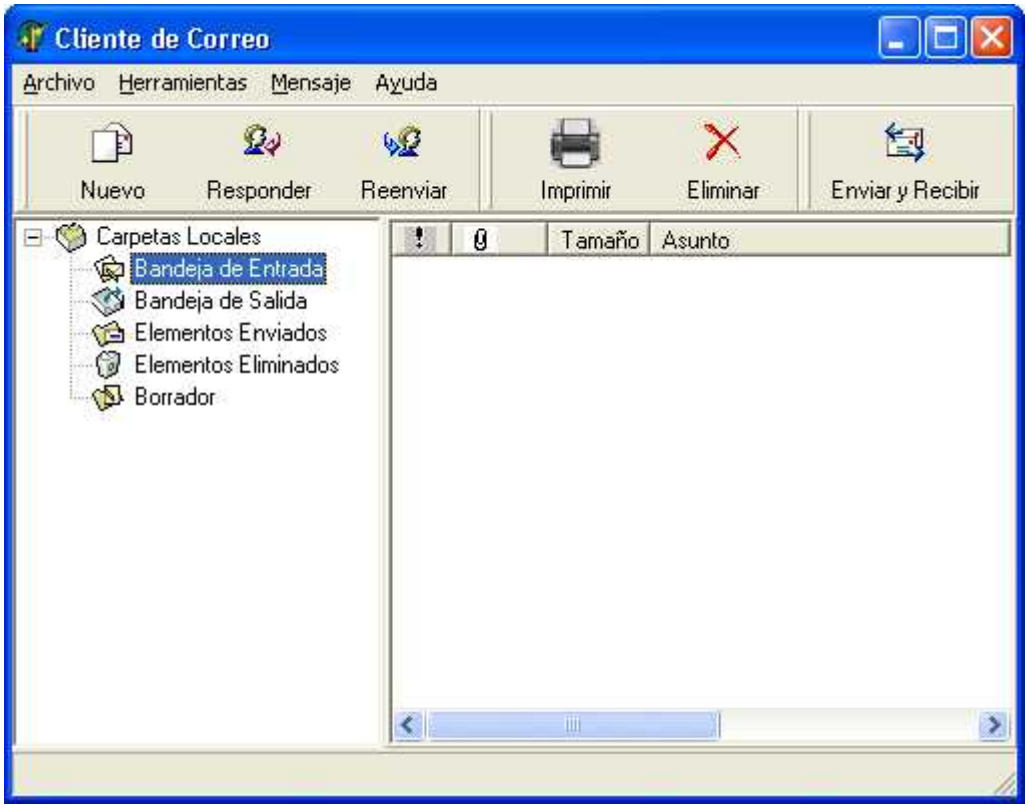


Figura No.1 Menú principal de Cliente de Correo

La ventana que aparece contiene un Menú principal y una Barra de acceso inmediato con las características propias de una ventana de manejo de correo. La estructura de menú Cliente de Correo da acceso a una serie de herramientas que ayudan a la gestión de correo electrónico. De igual manera la *barra de acceso inmediato* fue diseñada para ayudar a obtener con facilidad y rapidez algunas funciones que se representan en el menú principal.

Antes de poder trabajar con el *Cliente de Correo* se debe primeramente configurar la cuenta o buzón de correo que servirá para realizar cualquier tipo de acción de correo electrónico. Para poder configurar selecciono dentro del menú Herramientas y luego escojo la opción Cuentas, tal como se aprecia en la siguiente figura.

Figura No.2 Menu Herramientas / Cuentas

Una vez que escojo la opción Cuentas me aparece una ventana similar la de la Figura No. 3

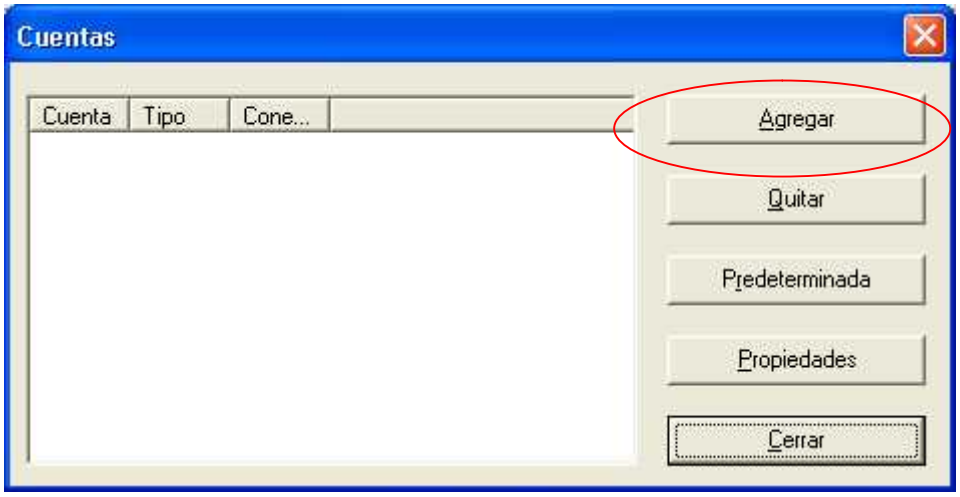


Figura No.3 Ventana de Configuración de las Cuentas

Una vez ubicados en la ventana de Configuración de Cuentas debo hacer un clic en el botón *Agregar* y entonces me aparecerá la ventana de Propiedades para poder ingresar los datos necesarios de la cuenta que se va a crear.

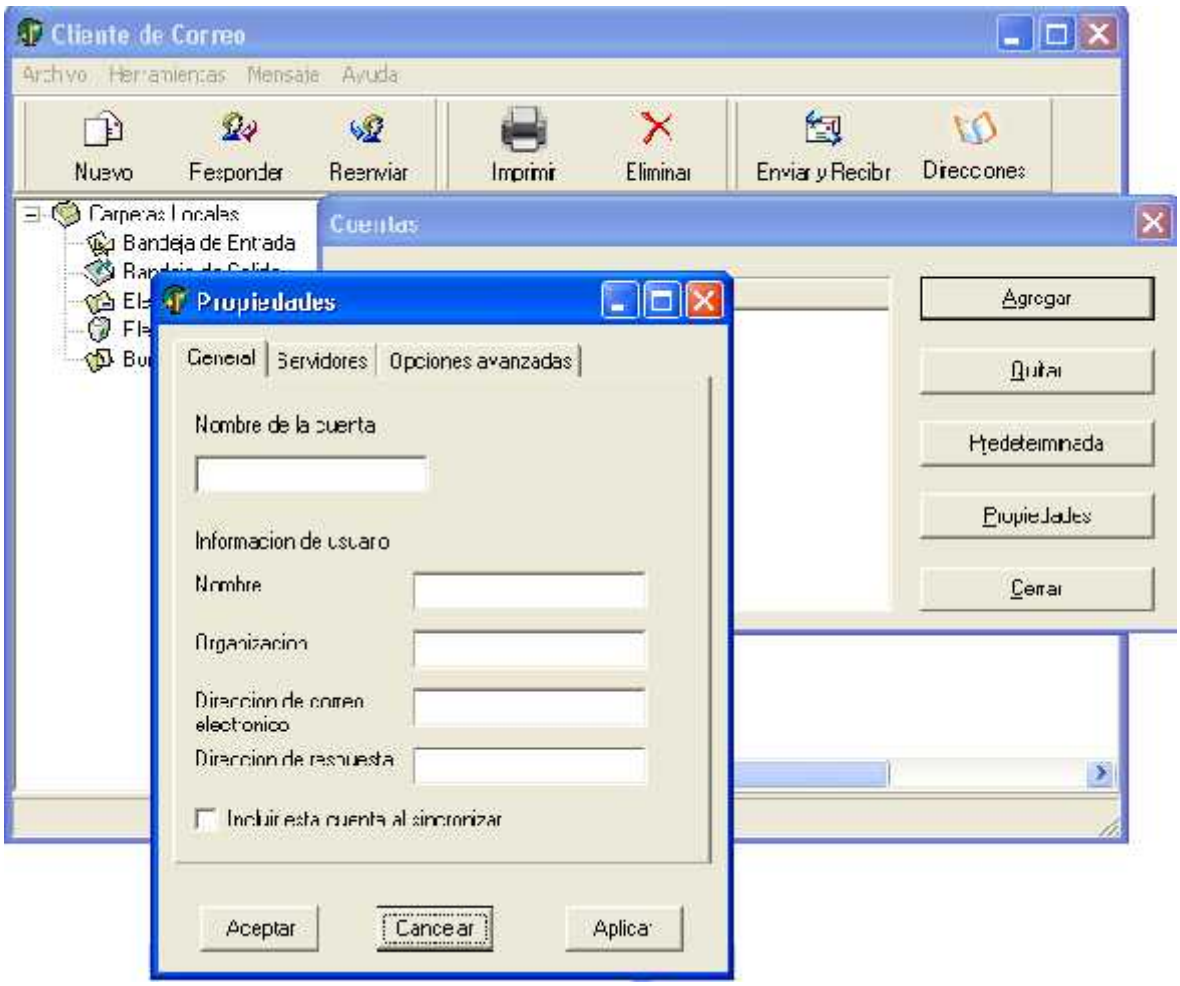


Figura No. 4 Ventana de Propiedades de una Cuenta de Correo

Procedemos entonces a llenar datos necesarios:

En la Pestaña General

Nombre de la Cuenta	Un nombre que haga referencia a la Cuenta (Ej. Andinanet)
Información de usuario	
Nombre	Identificación del usuario
Organización	Referencia de la Institución donde pertenece el usuario
Dirección de correo	Dirección electrónica con el que se identifica en Internet al Usuario.
Dirección de respuesta	Dirección electrónica al que se devolverá el correo.

En la Pestaña Servidores

Correo entrante (POP)	Servidor de Correo de donde se bajarán los e-mails
Correo saliente (SMTP)	Servidor de Correo por donde se tansmitirán los e-mails
Nombre de la cuenta	Nombre del buzón creado en el Servidor de Correo
Contraseña	Password para iniciar una sesión en el Servidor de Correo
Recordar la contraseña	Si se marca, interactuará pidiendo la contraseña.

En la Pestaña Opciones Avanzadas

Correo saliente (SMTP)	Número de Puerto del Servicio de SMTP
Correo entrante (POP)	Número de Puerto del Servicio POP
Nombre de la cuenta	Nombre del buzón creado en el Servidor de Correo
Tiempo de espera	Tiempo máximo en tratar de establecer una conexión

Una vez ingresados los datos se hace un clic en el botón *Aplicar* y luego en *Aceptar*, entonces se guarda la información de la cuenta para realizar las conexiones necesarias.
Se puede también Agregar una nueva cuenta, Quitar una cuenta una establecida y modificar los datos de una cuenta ya creada.

- **Icono Nuevo**

Permite crear nuevos mensajes de correo electrónico. Sirve para llenar los datos de envío de correo como: la dirección electrónica del destinatario, una dirección adicional (copia) si la hay, el asunto o título del correo, un archivo de texto que se desee incluir (es opcional), la prioridad del mensaje, encriptación del mensaje (opcional) y el cuerpo propiamente dicho del mensaje. Como lo demuestra la figura No. 2.

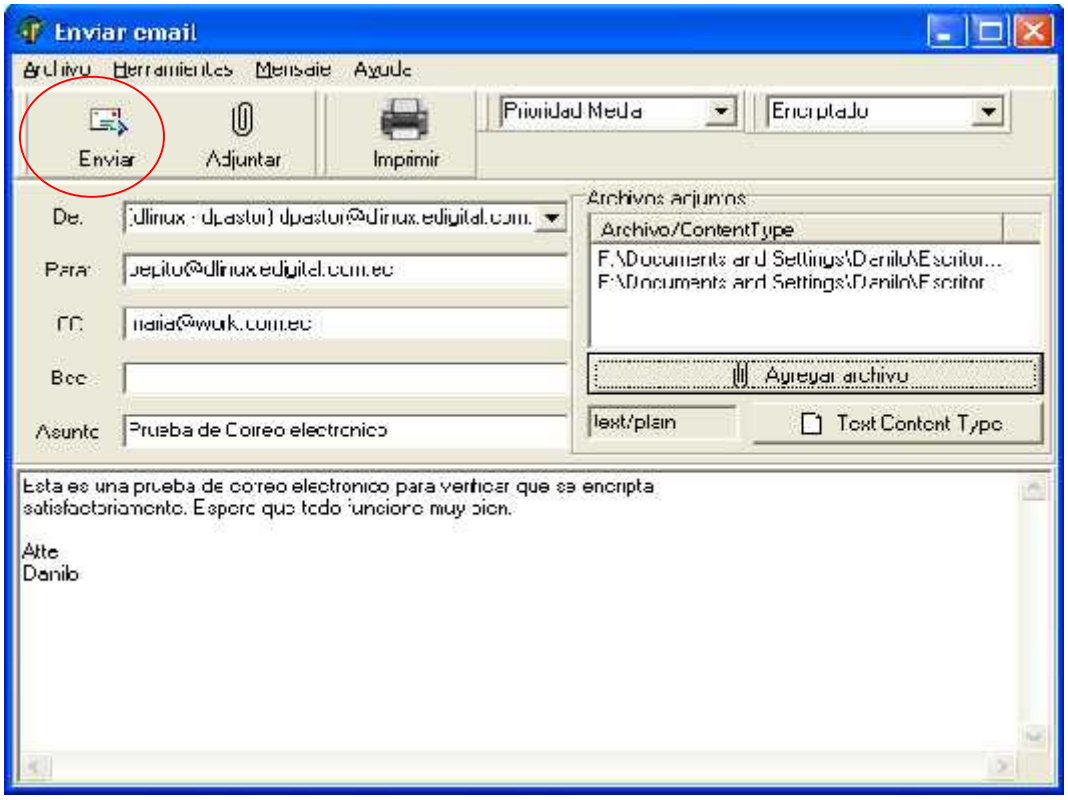


Figura No. 5 Ventana de creación de nuevo mail

Una vez que se finaliza de completar los datos del correo, que se este creando se hace un clic en el botón *enviar* ubicado en la barra de acceso inmediato y automáticamente se transferirá el mensaje al Servidor de Correo, indicando el correo enviado en la bandeja de salida y además mostrando en la barra de estado el mensaje “Enviando el mensaje”. Como se aprecia en la Figura No.4

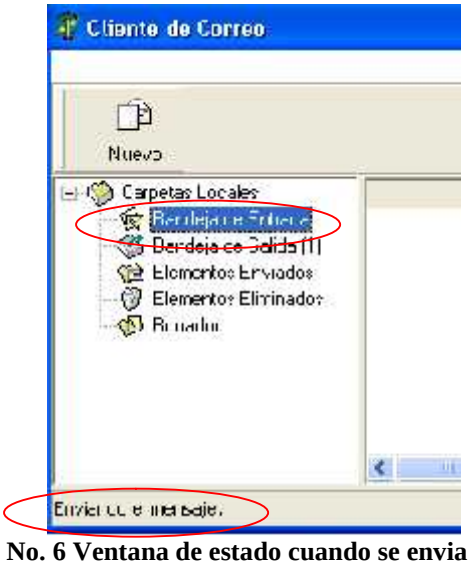


Figura No. 6 Ventana de estado cuando se envia un correo

- **Icono Responder o Reenviar**

Permite responder un mensaje que ha sido leído previamente a la persona que creo originalmente el mensaje. Me aparece la misma ventana que de Enviar correo, pero lleno el campo del Destinatario a cual se está respondiendo. De igual manera la opción Reenviar, funciona de forma similar a la opción Responder con la diferencia que se debe especificar en el destinatario la dirección del destinatario a cual voy a Reenviar el correo.

Figura No. 7 Responder o Reenviar un correo

- **Icono Eliminar**

Permite eliminar un mensaje de correo, pero directamente en el Servidor de Correo. Este paso se ejecuta previo al escoger el mail que se desee eliminar. Cuando se hace un clic en el botón *Eliminar* se borra el mensaje en el servidor y se refresca la parte de mensajes de correo.

- **Icono Enviar y Recibir**

Permite enviar mensajes de correo pendientes y primordialmente recibir los correos que están el en Servidor de Correo Entrante. Una vez que se hace un click aparecen una lista de todos los mensajes con la información solo de la cabecera, tal como lo muestra la Figura No. 8

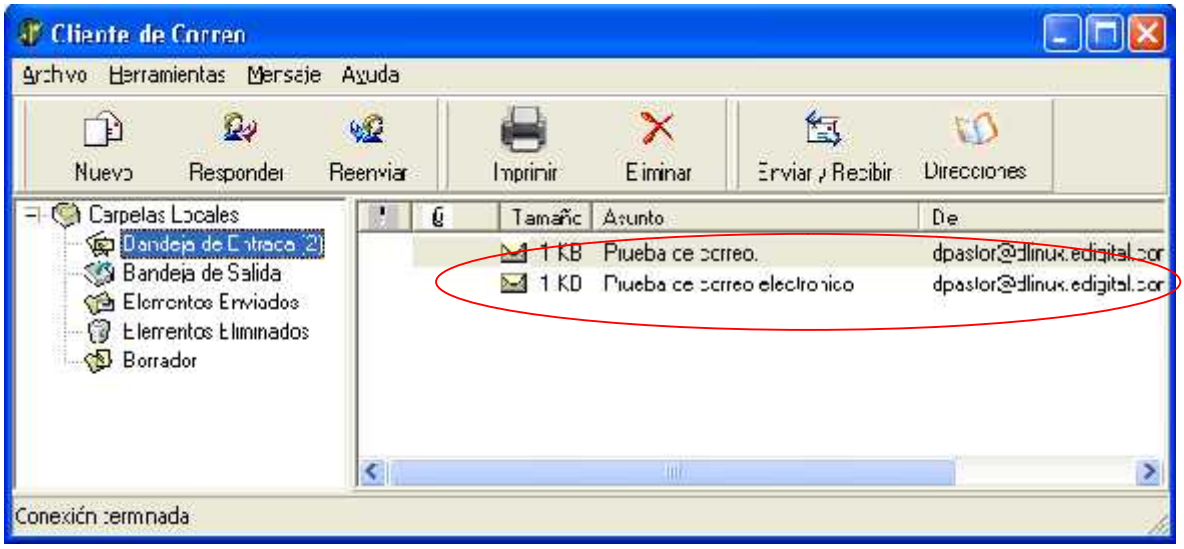


Figura No. 8 Mensajes recibidos

Luego se puede escoger el mensaje para poder observar su contenido, haciendo un click sobre el mail deseado. Esto produce, un nuevo espacio, en donde aparece el contenido del cuerpo del mensaje, tal como lo muestra en la Figura No. 9

Se puede ir observando el contenido de cada mensaje, haciendo un click en cualquiera de los mensajes listados en la parte superior, donde aparecen los mensajes recibidos.

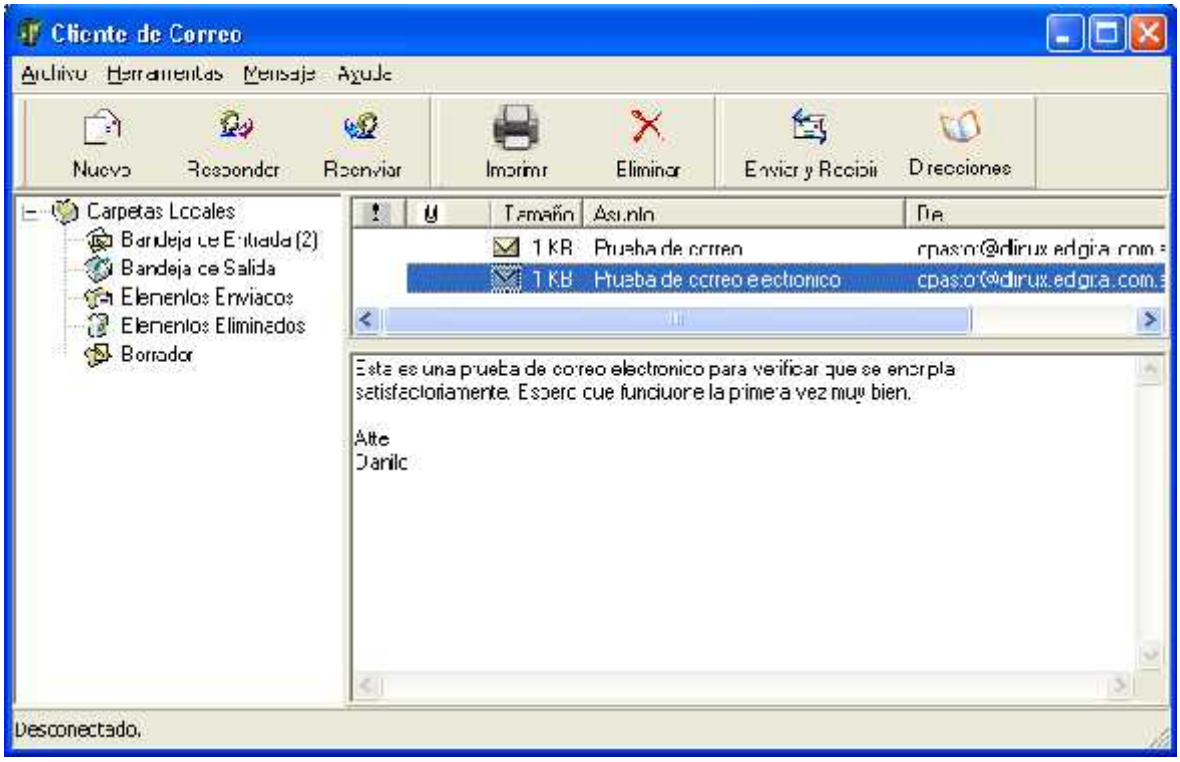


Figura No. 9 Mensajes recibidos con su contenido respectivo.

También se puede leer todas las características del mensaje haciendo un doble click sobre el mensaje deseado y nos aparcera una nueva ventana similar a la mostrada en la Figura No. 10

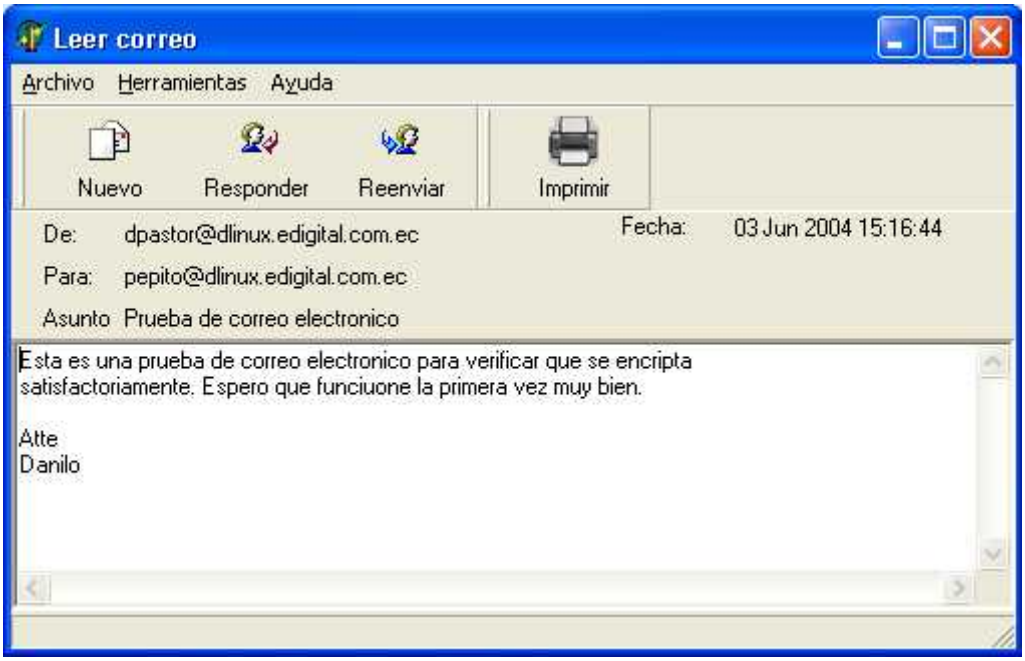


Figura No. 10 Ventana de Lectura de mensajes en forma detallada.

Como se muestra en la Figura se detalla tanto los campos de la cabecera como del cuerpo del mensaje y abre la posibilidad de Responder, Reenviar e Imprimir el actual mensaje mediante los botones de la barra de acceso inmediato.

Dentro de este menú Ayuda encontramos la opción de ***Acerca de..*** que indica la versión del *Cliente de Correo*.

ANEXO No. 3

CONTENIDO DE LOS ESTANDARES DE CORREO ELECTRONICO UTILIZADOS EN LA INVESTIGACION

RFC 821 – SIMPLE MAIL TRANFER PROTOCOL (SMTP)

RFC 821 August 1982
Simple Mail Transfer Protocol

TABLE OF CONTENTS

RFC 822 – BASIC MESSAGE FORMAT AND ENCODING

Standard for ARPA Internet Text Messages

TABLE OF CONTENTS

APPENDIX

RFC 1939 – POST OFFICE PROTOCOL (POP3)

Post Office Protocol - Version 3

Status of this Memo

This document specifies an Internet standards track protocol for the Internet community, and requests discussion and suggestions for improvements. Please refer to the current edition of the "Internet Official Protocol Standards" (STD 1) for the standardization state and status of this protocol. Distribution of this memo is unlimited.

Table of Contents

RFC 2045 – MULTIPURPOSE INTENET MAIL: FORMAT OF INTERNET MESSAGE BODIES

Internet mail header fields. The fourth document, RFC 2048, specifies various IANA registration procedures for MIME-related facilities. The fifth and final document, RFC 2049, describes MIME conformance criteria as well as providing some illustrative examples of MIME message formats, acknowledgements, and the bibliography.

These documents are revisions of RFCs 1521, 1522, and 1590, which themselves were revisions of RFCs 1341 and 1342. An appendix in RFC 2049 describes differences and changes from previous versions.

Table of Contents

ANEXO No. 4

CODIGO FUENTE DE GENERACION DE LA CLAVE

```
unit Codificador;

interface

uses
  SysUtils, DateUtils, IdGlobal, IniFiles;

type
  TCodificador = class
    private
      { Private declarations }
      fZonas : THashedStringList;
      fDominios : THashedStringList;
      fCompletamiento : string;
      function CodificarZonaHoraria(lZona : string) : string;
      function CodificarFecha(lFecha : string) : string;
      function CodificarHora(lHora : string) : string;
      function CodificarDireccion(lDireccion : string) : string;
      function CodificarDominio(lDominio : string) : string;
      function CodificarNumero(lValor : integer; lCantidadBits : integer) : string;
      procedure SetCompletamiento(lCompletamiento : string);
    public
      { Public declarations }
      constructor Create;
      destructor Free;
      function CodificarFechaHora(lFechaHora : string) : string;
      function CodificarRemitente(lDireccion : string) : string;
      function CodificarDestinatario(lDireccion : string; lTipoDestinatario : integer) : string;
      function CodificarPrioridad(lPrioridad : integer) : string;
      function CodificarAdjuntos(lAdjuntos : integer) : string;
      function CodificarAsunto(lAsunto : string) : string;
      function GetCompletamiento : string;
      function GenerarCodigo(lFechaHora : string; lRemitente: string; lDestinatario : string;
lTipoDestinatario : integer; lPrioridad : integer; lAdjuntos : integer; lAsunto : string) : string;
  end;

implementation

constructor TCodificador.Create;
var
  Codigo : string;
begin
  fCompletamiento := '';
  { ********************************************************************************** }
  { ******************** Codificación de fZonas Horarias ********************** }
  { ********************************************************************************** }
  fZonas := THashedStringList.Create;
  fZonas.CaseSensitive := false;
```

```
  Codigo := '000001';
  fZonas.AddObject('UT',TObject(Codigo));
  Codigo := '000010';
  fZonas.AddObject('GMT',TObject(Codigo));
   ……
   ……
  fDominios.AddObject('otros',TObject(Codigo));
  { ************************************************************************** }
  { ***************** Codificación de fDominios Geográficos ***************** }
  Codigo := '0000000100';
  fDominios.AddObject('af',TObject(Codigo));
  Codigo := '0000001000';
   ……
   ……
   ……
  Codigo := '1011001100';
  fDominios.AddObject('zw',TObject(Codigo));
end;

destructor TCodificador.Free;
begin
  fZonas.Free;
  fDominios.Free;
end;
function TCodificador.CodificarZonaHoraria(lZona : string) : string;
var
  Idx : integer;
begin
  Idx := fZonas.IndexOf(lZona);
  if (Idx = -1)
    then
      Idx := fZonas.IndexOf('UT');

  Result := string(fZonas.Objects[Idx]);
end;

function TCodificador.CodificarFecha(lFecha : string) : string;
var
  DiaSemana, DiaMes, Mes, Anno : string;
begin
  DiaSemana := CodificarNumero(DayOfTheWeek(StrToDate(lFecha)), 3); // 3 bits
//  DiaSemana :=
Copy(IntToBin(DayOfTheWeek(StrToDate(lFecha))),Length(IntToBin(DayOfTheWeek(StrToDat
e(lFecha))))-2,3);

  DiaMes := CodificarNumero(DayOfTheMonth(StrToDate(lFecha)), 6); // 6 bits
//  DiaMes :=
Copy(IntToBin(DayOfTheMonth(StrToDate(lFecha))),Length(IntToBin(DayOfTheMonth(StrToD
ate(lFecha))))-5,6);
  if ((StrToInt(IntToStr(DayOfTheMonth(StrToDate(lFecha)))) mod 2) <> 0)
    then
      DiaMes[1] := '1';
  Mes := CodificarNumero(MonthOfTheYear(StrToDate(lFecha)), 5); // 5 bits
```

```
//  Mes :=
Copy(IntToBin(MonthOfTheYear(StrToDate(lFecha))),Length(IntToBin(MonthOfTheYear(StrTo
Date(lFecha))))-4,5);
  if ((StrToInt(IntToStr(MonthOfTheYear(StrToDate(lFecha)))) mod 2) <> 0)
    then
      Mes[1] := '1';
  Anno := CodificarNumero(YearOf(StrToDate(lFecha)), 12); // 12 bits
//  Anno :=
Copy(IntToBin(YearOf(StrToDate(lFecha))),Length(IntToBin(YearOf(StrToDate(lFecha))))-
11,12);
  if ((StrToInt(IntToStr(YearOf(StrToDate(lFecha)))) mod 2) <> 0)
    then
      Anno[1] := '1';
  Result := DiaSemana + DiaMes + Mes + Anno;
end;

function TCodificador.CodificarHora(lHora : string) : string;
var
  Hora, Minuto, Segundo, ZonaHoraria : string;
begin
  Hora := CodificarNumero(HourOf(StrToTime(lHora)), 5); // 5 bits
  Minuto := CodificarNumero(MinuteOf(StrToTime(lHora)), 6); // 6 bits
  Segundo := CodificarNumero(SecondOf(StrToTime(lHora)), 6); // 6 bits

//  Hora :=
Copy(IntToBin(HourOf(StrToTime(lHora))),Length(IntToBin(HourOf(StrToTime(lHora))))-4,5);
//  Minuto :=
Copy(IntToBin(MinuteOf(StrToTime(lHora))),Length(IntToBin(MinuteOf(StrToTime(lHora))))-
5,6);
//  Segundo :=
Copy(IntToBin(SecondOf(StrToTime(lHora))),Length(IntToBin(SecondOf(StrToTime(lHora))))-
5,6);
  ZonaHoraria := CodificarZonaHoraria('GMT'); // 6 bits
  Result := Hora + Minuto + Segundo + ZonaHoraria;
end;

function TCodificador.CodificarDominio(lDominio : string) : string;
var
  Idx : integer;
begin
  Idx := fDominios.IndexOf(lDominio);
  if (Idx = -1)
    then
      Idx := fDominios.IndexOf('otros');
  Result := string(fDominios.Objects[Idx]);
end;

function TCodificador.CodificarFechaHora(lFechaHora : string) : string;
var
  lFecha, lHora : string;
  cFecha, cHora : string;
begin
  lFecha := Copy(lFechaHora, 0, Pos(' ', lFechaHora)-1);
  lHora := Copy(lFechaHora, Pos(' ', lFechaHora)+1, Length(lFechaHora));
```

```
  cFecha := CodificarFecha(lFecha); // 26 bits
  cHora := CodificarHora(lHora); // 23 bits
  fCompletamiento := Copy((cFecha + cHora), 0, 28); // 28 bits
  Result := cFecha + cHora;
end;

function TCodificador.CodificarDireccion(lDireccion : string) : string;
var
  CantCarUsuario, CantDominios : integer;
  CantCarUsuarioStr, CantDominiosStr, Dominio : string;
begin
  CantCarUsuario := Pos('@', lDireccion) - 1;
  CantDominios := 1;
  while (Pos('.', lDireccion) <> 0) do
    begin
      Inc(CantDominios);
      lDireccion := Copy(lDireccion, Pos('.', lDireccion) + 1, Length(lDireccion) - Pos('.', lDireccion)
+ 1);
    end;
//  CantCarUsuarioStr := Copy(IntToBin(CantCarUsuario), Length(IntToBin(CantCarUsuario))-
4,5);
//  CantDominiosStr := Copy(IntToBin(CantDominios), Length(IntToBin(CantDominios))-2,3);
  CantCarUsuarioStr := CodificarNumero(CantCarUsuario, 5);
  CantDominiosStr := CodificarNumero(CantDominios, 3);
  Dominio := CodificarDominio(lDireccion);
  Result := CantCarUsuarioStr + CantDominiosStr + Dominio;
end;

function TCodificador.CodificarNumero(lValor : integer; lCantidadBits : integer) : string;
begin
  Result := Copy(IntToBin(lValor),Length(IntToBin(lValor))-(lCantidadBits-1),lCantidadBits)
end;

function TCodificador.CodificarPrioridad(lPrioridad : integer) : string;
begin
  Result := CodificarNumero(lPrioridad, 2);
end;

function TCodificador.CodificarAdjuntos(lAdjuntos : integer) : string;
begin
  Result := CodificarNumero(lAdjuntos, 2);
end;

function TCodificador.CodificarAsunto(lAsunto : string) : string;
begin
  Result := CodificarNumero(Length(lAsunto), 8);
end;

procedure TCodificador.SetCompletamiento(lCompletamiento : string);
begin
  fCompletamiento := lCompletamiento;
end;
```

```
function TCodificador.GetCompletamiento : string;
begin
  Result := fCompletamiento;
end;

function TCodificador.CodificarRemitente(lDireccion : string) : string;
begin
  Result := CodificarDireccion(lDireccion);
end;

function TCodificador.CodificarDestinatario(lDireccion : string; lTipoDestinatario : integer) :
string;
begin
  // Determinar lo del tipo de destinatario
  Result := CodificarDireccion(lDireccion) + CodificarNumero(lTipoDestinatario, 3);
end;

function TCodificador.GenerarCodigo(lFechaHora : string; lRemitente: string; lDestinatario :
string; lTipoDestinatario : integer; lPrioridad : integer; lAdjuntos : integer; lAsunto : string) : string;
var
  CodigoOriginal : string[128];
  CodigoPermutado : string[128];
  cFechaHora, cRemitente, cDestinatario, cPrioridad, cAsunto, cAdjuntos : string;
  CodigoGenerado : string[128];
  i : integer;
begin
  cFechaHora := CodificarFechaHora(lFechaHora); // 49 bits
  cRemitente := CodificarRemitente(lRemitente); // 18 bits
  cDestinatario := CodificarDestinatario(lDestinatario, lTipoDestinatario); // 21 bits
  cPrioridad := CodificarPrioridad(lPrioridad); // 2 bits
  cAdjuntos := CodificarAdjuntos(lAdjuntos); // 2 bits
  cAsunto := CodificarAsunto(lAsunto); // 8 bits
  // 49 + 18 + 21 + 2 + 2 + 8 + 28 = 128 bits en clave
  CodigoOriginal :=   cFechaHora + cRemitente + cDestinatario + cPrioridad + cAdjuntos +
cAsunto + fCompletamiento;
  // Permutamos 25 bits a la derecha
  CodigoPermutado := Copy(CodigoOriginal, Length(CodigoOriginal)-25, 25) +
Copy(CodigoOriginal, 0, Length(CodigoOriginal)-25);
  CodigoGenerado := CodigoOriginal;
  // Efectuamos el XOR entre el codigo original y el codigo permutado
  for i:=1 to 128 do
    if (CodigoOriginal[i] = CodigoPermutado[i])
      then
        CodigoGenerado[i] := '0'
      else
        CodigoGenerado[i] := '1';

  Result := CodigoGenerado;
end;
end.
```